

Cisco IOS Voice Command Reference - S commands

First Published: 2015-08-04

Last Modified: 2026-09-29

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED “AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

All printed copies and duplicate soft copies of this document are considered uncontrolled. See the current online version for the latest version.

Cisco has more than 200 offices worldwide. Addresses and phone numbers are listed on the Cisco website at www.cisco.com/go/offices.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: https://www.cisco.com/c/en/us/about/legal/trademarks.html. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1721R)

© 2026 Cisco Systems, Inc. All rights reserved.



CONTENTS

CHAPTER 1 **sccp through service-type call-check** 1

- sccp 3
- sccp blf-speed-dial retry-interval 5
- sccp ccm 6
- sccp ccm group 9
- sccp codec mask 11
- sccp ip precedence 13
- sccp local 14
- sccp plar 16
- sccp switchback timeout guard 17
- scenario-cause 18
- sdspfarm tag 20
- sdspfarm transcode sessions 22
- sdspfarm units 23
- secondary 24
- secure-ciphersuite 27
- security 29
- security acl 31
- security izct 32
- security mode 34
- sequence-numbers 36
- server (auto-config application) 38
- server (presence) 39
- server (RLM) 41
- server absent reject 43
- server flow-control 44

server registration-port 47
server routing 49
server trigger arq 50
server trigger brq 53
server trigger drq 56
server trigger irr 59
server trigger lcf 62
server trigger lrj 65
server trigger lrq 68
server trigger rai 71
server trigger rrq 74
server trigger urq 77
service 80
service dsapp 82
service-flow primary upstream 88
service-map 89
service-relationship 90
service-type call-check 91

CHAPTER 2 **session through sgcp tse payload** 93
session 95
session group 96
session protocol (dial peer) 97
session protocol (Voice over Frame Relay) 99
session protocol aal2 101
session protocol multicast 102
session refresh 103
session start 104
session target (MMoIP dial peer) 106
session target (POTS dial peer) 109
session target (VoATM dial peer) 110
session target (VoFR dial peer) 113
session target (VoIP dial peer) 115
session target 120

session transport 121
session transport (H.323 voice-service) 123
session transport (SIP) 124
session-set 126
session-timeout 127
set 128
set http client cache stale 130
set pstn-cause 131
set sip-status 134
settle-call 137
settlement 138
settlement roam-pattern 140
sgcp 141
sgcp call-agent 143
sgcp graceful-shutdown 145
sgcp max-waiting-delay 147
sgcp modem passthru 149
sgcp quarantine-buffer disable 151
sgcp request retries 153
sgcp request timeout 155
sgcp restart 157
sgcp retransmit timer 159
sgcp timer 161
sgcp tse payload 163
source filter 165

CHAPTER 3 **show aal2 profile through show call filter match-list** 167
show aal2 profile 168
show app-hosting detail 170
show atm video-voice address 172
show auto-config 173
show backhaul-session-manager group 175
show backhaul-session-manager session 178
show backhaul-session-manager set 180

show call accounting-template voice 181
show call active fax 184
show call active media 194
show call active total-calls 202
show call active video 203
show call active voice 214
show call application app-level 237
show call application gateway-level 241
show call application interface 244
show call application services registry 248
show call application session-level 250
show call application sessions 262
show call application voice 265
show call fallback cache 271
show call fallback config 273
show call fallback stats 275
show call filter components 277
show call filter match-list 279

CHAPTER 4 **show call history fax through show debug condition** 281
show call history fax 283
show call history media 293
show call history stats 302
show call history video 311
show call history video record 313
show call history voice 314
show call history watermark connected table 320
show call language voice 322
show call leg 324
show call media forking 329
show callmon 330
show call prompt-mem-usage 332
show call resource voice stats 335
show call resource voice threshold 337

show call rsvp-sync conf 339
show call rsvp-sync stats 341
show call spike status 343
show call threshold 345
show call treatment 347
show call-router routes 350
show call-router status 352
show ccm-manager 355
show cdapi 365
show ces clock-select 367
show connect 368
show controllers rs366 370
show controllers timeslots 372
show controllers voice 374
show crm 377
show csm 379
show csm call 386
show cube debug category codes 388
show cube status 389
show debug condition 392

CHAPTER 5 **show dial-peer through show gatekeeper zone prefix** 395
show dial-peer 396
show dial-peer video 397
show dial-peer voip keepalive status 398
show dial-peer voice 400
show dialplan dialpeer 411
show dialplan incall 417
show dialplan incall uri 420
show dialplan in-carrier 426
show dialplan in-trunk-group-label 428
show dialplan number 430
show dialplan uri 433
show dn-numbers 435

show dspfarm 437
show dspfarm profile 445
show dsp-group 448
show echo-cancel 450
show event-manager consumers 452
show frame-relay vofr 454
show gatekeeper calls 456
show gatekeeper circuits 458
show gatekeeper cluster 460
show gatekeeper endpoint circuits 461
show gatekeeper endpoints 463
show gatekeeper gw-type-prefix 466
show gatekeeper performance statistics 468
show gatekeeper servers 472
show gatekeeper status 474
show gatekeeper status cluster 476
show gatekeeper zone cluster 477
show gatekeeper zone prefix 478
show gatekeeper zone status 480

CHAPTER 6 **show gateway through show modem relay statistics** 483
show gateway 484
show h323 calls preserved 486
show h323 gateway 488
show h323 gateway prefixes 494
show http client cache 496
show http client cache 500
show http client cookie 503
show http client history 504
show http client secure status 505
show http client statistics 507
show interface dspfarm 510
show interfaces cable-modem 515
show ip address trusted check 519

show iua as 520
show iua asp 523
show media-proxy sessions 525
show media resource status 529
show mediacard 530
show mgcp 533
show mgcp connection 542
show mgcp endpoint 546
show mgcp nas 549
show mgcp profile 553
show mgcp srtp 557
show mgcp statistics 560
show modem relay statistics 564

CHAPTER 7 **show mrcp client session active through show sip dhcp** 569
show monitor event-trace voip ccsip (EXEC) 571
show mrcp client session active 588
show mrcp client session history 591
show mrcp client statistics hostname 595
show mwi relay clients 597
show nextport 598
show nextport vpd 604
show num-exp 606
show piafs status 608
show platform hardware qfp active feature sbc fork global 610
show platform hardware qfp active feature sbc fork session 612
show pots csm 615
show pots status 616
show pots volume 620
show presence global 621
show presence subscription 623
show proxy h323 calls 627
show proxy h323 detail-call 628
show proxy h323 status 633

show raw 634
show rawmsg 636
show rlm group statistics 638
show rlm group status 641
show rlm group timer 643
show rpms-proc counters 645
show running-config dial-peer 647
show rtpspi 649
show rtsp client session 651
show rudpv0 failures 654
show rudpv0 statistics 656
show rudpv1 658
show sccp 661
show sccp ccm group 668
show sccp connections details 670
show sccp connections internal 671
show sccp connections rsvp 672
show sccp connections summary 674
show sccp server statistics 676
show sdspfarm 677
show settlement 683
show sgcp connection 685
show sgcp endpoint 687
show sgcp statistics 688
show shared-line 690
show sip dhcp 692

CHAPTER 8 **show sip service through show trunk hdlc** 695

show sip service 697
show sip-ua calls 698
show sip-ua connections 713
show sip-ua map 721
show sip-ua min-se 724
show sip-ua mwi 725

show sip-ua register status 727
show sip-ua retry 729
show sip-ua service 731
show sip-ua srtp 733
show sip-ua statistics 735
show sip-ua status 744
show sip-ua status refer-ood 748
show sip-ua timers 750
show spe voice 753
show ss7 mtp1 channel-id 756
show ss7 mtp1 links 759
show ss7 mtp2 ccb 762
show ss7 mtp2 state 765
show ss7 mtp2 stats 768
show ss7 mtp2 timer 772
show ss7 mtp2 variant 774
show ss7 sm session 776
show ss7 sm set 778
show ss7 sm stats 781
show stcapp buffer-history 783
show stcapp device 785
show stcapp feature codes 792
show stcapp statistics 796
show subscription 798
show subscription local 804
show tbct 809
show tdm mapping 810
show tgrep neighbors 812
show translation-rule 814
show trunk group 817
show trunk hdlc 821

CHAPTER 9 **show vdev through show voice statistics memory-usage** 823
show vdev 825

show vfc 827
show vfc cap-list 828
show vfc default-file 829
show vfc directory 830
show vfc version 832
show video call summary 835
show voice accounting method 836
show voice accounting response pending 838
show voice busyout 839
show voice cable-status 840
show voice call 841
show voice call rate 851
show voice cause-code 853
show voice class called-number 855
show voice class called-number-pool 856
show voice class e164-pattern-map 858
show voice class e164-translation 859
show voice class phone-proxy 861
show voice class resource-group 863
show voice class server-group 865
show voice class sip-options-keepalive 867
show voice class sip-predefined-profiles 868
show voice class uri 869
show voice connectivity summary 872
show voice data 873
show voice dnis-map 875
show voice dsmp stream 877
show voice dsp 884
show voice dsp channel 892
show voice dsp crash-dump 895
show voice dsp summary 897
show voice eddri prefix 899
show voice emergency locations 900
show voice enum-match-table 901

show voice hpi capture 902
show voice iec description 903
show voice lmr 904
show voice pcm capture 909
show voice port 910
show voice sip license 922
show voice source-group 957
show voice statistics csr interval accounting 960
show voice statistics csr interval aggregation 962
show voice statistics csr since-reset accounting 967
show voice statistics csr since-reset aggregation-level 969
show voice statistics csr since-reset all 974
show voice statistics iec 978
show voice statistics interval-tag 980
show voice statistics memory-usage 982

CHAPTER 10 **show voice trace through shutdown (voice-port) 985**

show voice trace 987
show voice translation-profile 988
show voice translation-rule 990
show voice trunk-conditioning signaling 992
show voice trunk-conditioning supervisory 995
Show voice vrf 998
show voice vtsp 999
show voip debug version 1001
show voip fpi call-rate 1002
show voip fpi calls 1003
show voip fpi rtts 1010
show voip fpi stats 1011
show voip htsp 1017
show voip recmsp session 1019
show voip rtp connections 1021
show voip rtp forking 1029
show voip rtp stats 1031

show voip stream-service callid 1035
show voip stream-service connection 1037
show voip stream-service connection history 1039
show voip stream-service connection id 1041
show voip stream-service server 1044
show voip stream-service statistics 1046
show voip trace 1048
show voip trunk group 1056
show vrm active_calls 1057
show vrm vdevices 1060
show vsp 1071
show wsapi 1076
show xcsp port 1080
show xcsp slot 1082
shut 1083
shutdown (Annex G neighbor) 1084
shutdown (Annex G) 1085
shutdown (dial-peer) 1086
shutdown (DSP Farm profile) 1087
shutdown (gatekeeper) 1088
shutdown (gateway) 1089
shutdown (mediacard) 1090
shutdown (auto-config application) 1091
shutdown (RLM) 1092
shutdown (settlement) 1093
shutdown (trace) 1095
shutdown (voice-port) 1097

CHAPTER 11 **signal through srv version** 1099
signal 1101
signal did 1105
signal keepalive 1106
signal pattern 1108
signal sequence oos 1111

signal timing idle suppress-voice 1113
signal timing oos 1116
signal timing oos restart 1118
signal timing oos standby 1120
signal timing oos suppress-all 1122
signal timing oos suppress-voice 1124
signal timing oos timeout 1126
signaling forward 1128
signaling forward (dial peer) 1133
signal-type 1138
silent-discard untrusted 1140
silent-fax 1141
sip 1142
sip-header 1144
sip-header SIP-StatusLine 1145
sip-server 1146
sip-ua 1148
sni send (voice class) 1151
snmp enable peer-trap dscp-profile 1152
snmp enable peer-trap poor-qov 1153
snmp-server enable traps voice (DSCP profile) 1154
soft-offhook 1155
source-address (uc-wsapi) 1157
source carrier-id 1158
source filter 1159
source-ip (media-profile) 1160
source trunk-group-label 1161
speed dial 1162
srtp (dial peer) 1165
srtp (voice) 1167
srtp-auth 1169
srtp-crypto 1171
srtp negotiate 1173
srv version 1175

CHAPTER 12 ss7 mtp2-variant through switchover method 1177

ss7 mtp2-variant 1179

ss7 mtp2-variant bellcore 1184

ss7 mtp2-variant itu 1186

ss7 mtp2-variant ntt 1188

ss7 mtp2-variant ttc 1190

ss7 mtp2-variant itu-white 1192

ss7 session 1194

ss7 session cumack_t 1197

ss7 session kp_t 1199

ss7 session m_cumack 1201

ss7 session m_outseq 1203

ss7 session m_rcvnum 1205

ss7 session m_retrans 1207

ss7 session retrans_t 1209

ss7 set 1211

ss7 set failover-timer 1213

station-id name 1214

station-id number 1216

stats 1218

stcapp 1219

stcapp call-control mode 1221

stcapp feature callback 1223

stcapp ccm-group 1224

stcapp feature access-code 1225

stcapp feature callback 1227

stcapp feature speed-dial 1228

stcapp register capability 1230

stcapp security mode 1232

stcapp security trustpoint 1234

stcapp supplementary-services 1236

stcapp timer 1237

stream-service profile 1238

stun 1239
stun flowdata agent-id 1240
stun flowdata catlife 1241
stun flowdata keepalive 1242
stun flowdata shared-secret 1244
stun usage firewall-traversal flowdata 1246
stun usage ice lite 1247
subaddress 1248
subcell-mux 1249
subscription asnl session history 1250
subscription maximum 1251
supervisory answer dualtone 1252
supervisory custom-cptone 1254
supervisory disconnect 1256
supervisory disconnect anytone 1257
supervisory disconnect dualtone 1259
supervisory disconnect dualtone voice-class 1261
supervisory disconnect lcfo 1263
supervisory dualtone-detect-params 1264
supervisory sit us 1266
supplementary-service h225-notify cid-update (dal peer) 1269
supplementary-service h225-notify cid-update (voice-service) 1271
supplementary-service h450.2 (dial peer) 1273
supplementary-service h450.2 (voice-service) 1274
supplementary-service h450.3 (dial peer) 1275
supplementary-service h450.3 (voice-service) 1276
supplementary-service h450.7 1277
supplementary-service h450.12 (dial peer) 1279
supplementary-service h450.12 (voice-service) 1280
supplementary-service media-renegotiate 1282
supplementary-service qsig call-forward 1283
supplementary-service sip 1285
supported language 1288
suppress 1290

survivability single-register 1291
suspend-resume (SIP) 1292
switchback interval 1293
switchback method 1294
switchover method 1296



sccp through service-type call-check

- sccp, on page 3
- sccp blf-speed-dial retry-interval, on page 5
- sccp ccm, on page 6
- sccp ccm group, on page 9
- sccp codec mask, on page 11
- sccp ip precedence, on page 13
- sccp local, on page 14
- sccp plar, on page 16
- sccp switchback timeout guard, on page 17
- scenario-cause, on page 18
- sdspfarm tag, on page 20
- sdspfarm transcode sessions, on page 22
- sdspfarm units, on page 23
- secondary, on page 24
- secure-ciphersuite, on page 27
- security, on page 29
- security acl, on page 31
- security izct, on page 32
- security mode, on page 34
- sequence-numbers, on page 36
- server (auto-config application), on page 38
- server (presence), on page 39
- server (RLM), on page 41
- server absent reject, on page 43
- server flow-control, on page 44
- server registration-port, on page 47
- server routing, on page 49
- server trigger arq, on page 50
- server trigger brq, on page 53
- server trigger drq, on page 56
- server trigger irr, on page 59
- server trigger lcf, on page 62
- server trigger lrj, on page 65

- server trigger lrq, on page 68
- server trigger rai, on page 71
- server trigger rrq, on page 74
- server trigger urq, on page 77
- service, on page 80
- service dsapp, on page 82
- service-flow primary upstream, on page 88
- service-map, on page 89
- service-relationship, on page 90
- service-type call-check, on page 91

sccp

Note The documentation set for this product strives to use bias-free language. For purposes of this documentation set, bias-free is defined as language that does not imply discrimination based on age, disability, gender, racial identity, ethnic identity, sexual orientation, socioeconomic status, and intersectionality. Exceptions may be present in the documentation due to language that is hardcoded in the user interfaces of the product software, language used based on RFP documentation, or language that is used by a referenced third-party product.

To enable the Skinny Client Control Protocol (SCCP) protocol and its related applications (transcoding and conferencing), use the **sccp** command in global configuration mode. To disable the protocol, use the **no** form of this command.

sccp
no sccp

Syntax Description

This command has no arguments or keywords.

Command Default

Disabled

Command Modes

Global configuration (config)

Command History

Release	Modification
12.1(5)YH	This command was introduced on the Cisco VG200.
12.2(13)T	This command was implemented on the Cisco 2600 series, Cisco 3620, Cisco 3640, Cisco 3660, and Cisco 3700 series.

Usage Guidelines

The router on which this command is used must be equipped with one or more digital T1/E1 packet voice trunk network modules (NM-HDVs) or high-density voice (HDV) transcoding/conferencing DSP farms (NM-HDV-FARMs) to provide digital-signal-processor (DSP) resources.

SCCP and its related applications (transcoding and conferencing) become enabled only if digital-signal-processor (DSP) resources for these applications are configured, DSP-farm service is enabled, and the Cisco CallManager registration process is completed.

The **no** form of this command disables SCCP and its applications by unregistering from the active Cisco CallManager, dropping existing connections, and freeing allocated resources.

Examples

The following example sets related values and then enables SCCP:

```
Router(config)# sccp ccm 10.10.10.1 priority 1
Router(config)# sccp local fastEthernet 0/0
Router(config)# sccp switchback timeout guard 180
Router(config)# sccp ip precedence 5
Router(config)# sccp
Router(config)# end
```

Related Commands

Command	Description
dspfarm (DSP farm)	Enables DSP-farm service.
show dspfarm	Displays summary information about DSP resources.
show sccp	Displays the SCCP configuration information and current status.

sccp blf-speed-dial retry-interval

To set the retry timeout for Busy Lamp Field (BLF) notification for speed-dial numbers on SCCP phones registered to an external Cisco Unified CME router, use the **sccp blf-speed-dial retry-interval**command in presence configuration mode. To reset to the default, use the **no** form of this command.

sccp blf-speed-dial retry-interval *seconds* **limit** *number*
no sccp blf-speed-dial retry-interval

Syntax Description

seconds	Retry timeout in seconds. Range: 60 to 3600. Default: 60.
limit *number*	Maximum number of retries. Range: 10 to 100. Default: 10.

Command Default

Retry timeout is 60 seconds; retry limit is 10.

Command Modes

Presence configuration (config-presence)

Command History

Cisco IOS Release	Modification
12.4(11)XJ	This command was introduced.
12.4(15)T	This command was integrated into Cisco IOS Release 12.4(15)T.

Usage Guidelines

This command specifies how frequently the router attempts to subscribe for the line status of an external directory number when the BLF speed-dial feature is configured on a SCCP phone. This retry mechanism is used when either the presentity does not exist or the router receives a terminated NOTIFY from the external presence server. If the subscribe request toward the external server fails after the configured number of retries, the subscribe request from the phone is rejected.

Examples

The following example shows the BLF speed-dial retry interval set to 100 seconds and the limit to 25:

```
Router(config)# presence
Router(config-presence)# sccp blf-speed-dial retry-interval 100 limit 25
```

Related Commands

Command	Description
allow subscribe	Allows internal watchers to monitor external presence entities (directory numbers).
blf-speed-dial	Enables BLF monitoring for a speed-dial number on a phone registered to Cisco Unified CME.
server	Specifies the IP address of a presence server for sending presence requests from internal watchers to external presence entities.
show presence global	Displays configuration information about the presence service.

sccp ccm

To add a Cisco Unified Communications Manager server to the list of available servers and set various parameters--including IP address or Domain Name System (DNS) name, port number, and version number--use the **sccp ccm** command in global configuration mode. To remove a particular server from the list, use the **no** form of this command.

NM-HDV or NM-HDV-FARM Voice Network Modules
sccp ccm {*ipv4-addressipv6-addressdns*} **priority** *priority* [**port** *port-number*] [**version** *version-number*] [**trustpoint** *label*]
no sccp ccm {*ipv4-addressipv6-addressdns*}

NM-HDV2 or NM-HD-1V/2V/2VE Voice Network Modules
sccp ccm {*ipv4-addressipv6-addressdns*} **identifier** *identifier-number* [**priority** *priority*] [**port** *port-number*] [**version** *version-number*] [**trustpoint** *label*]
no sccp ccm {*ipv4-addressipv6-addressdns*}

Syntax Description

ipv4 -address	IPv4 address of the Cisco Unified Communications Manager server.
ipv6-address	IPv6 address of the Cisco Unified Communications Manager server.
dns	DNS name.
identifier *identifier-number*	Specifies the number that identifies the Cisco Unified Communications Manager server. The range is 1 to 65535.
priority *priority*	Specifies the priority of this Cisco Unified Communications Manager server relative to other connected servers. The range is 1 (highest) to 4 (lowest). **Note** This keyword is required only for NM-HDV and NM-HDV-FARM modules. Do not use this keyword if you are using the NM-HDV2 or NM-HD-1V/2V/2VE; set the priority using the **associate ccm** command in the Cisco Unified Communications Manager group.
port *port -number*	(Optional) Specifies the TCP port number. The range is 1025 to 65535. The default is 2000.
version *version -number*	(Optional) Cisco Unified Communications Manager version. Valid versions are **3.0**, **3.1**, **3.2**, **3.3**, **4.0**, **4.1**, **5.0.1**, **6.0**, and **7.0+**. There is no default value.
trustpoint	(Optional) Specifies the trustpoint for Cisco Unified Communications Manager certificate.
label	Cisco Unified Communications Manager trustpoint label.

Command Default

The default port number is 2000.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.1(5)YH	This command was introduced.
12.3(8)T	This command was modified. The **identifier** keyword and additional values for Cisco Unified Communications Manager versions were added.
12.4(11)XW	This command was modified. The **6.0** keyword was added to the list of version values.
12.4(20)T	This command was integrated into Cisco IOS Release 12.4(20)T.
12.4(22)T	This command was modified. Support for IPv6 was added. The **version** keyword and *version-number*argumentwere changed from being optional to being required, and the **7.0+** keyword was added.
15.0(1)M	This command was modified in a release earlier than Cisco IOS Release 15.0(1)M. The **trustpoint**keyword and the *label* argument were added.

Usage Guidelines

You can configure up to four Cisco Unified Communications Manager servers--a primary and up to three backups--to support digital signal processor (DSP) farm services. To add the Cisco Unified Communications Manager server to a Cisco Unified Communications Manager group, use the **associate ccm** command.

IPv6 support is provided for registration with Cisco Unified CM version 7.0 and later.

To enable Ad Hoc or Meet-Me hardware conferencing in Cisco Unified CME, you must first set the **version** keyword to **4.0** or a later version.

Beginning with Cisco IOS Release 12.4(22)T users manually configuring the **sccp ccm**command must provide the version. Existing router configurations are not impacted because automatic upgrade and downgrade are supported.

Examples

The following example shows how to add the Cisco Unified Communications Manager server with IP address 10.0.0.0 to the list of available servers:

```
Router(config)# sccp ccm 10.0.0.0 identifier 3 port 1025 version 4.0
```

The following example shows how to add the Cisco Unified CallManager server whose IPv6 address is 2001:DB8:C18:1::102:

```
Router(config)# sccp ccm 2001:DB8:C18:1::102 identifier 2 version 7.0
```

Related Commands

Command	Description
associate ccm	Associates a Cisco Unified Communications Manager server with a Cisco Unified Communications Manager group and establishes its priority within the group.
sccp	Enables SCCP and its associated transcoding and conferencing applications.
sccp ccm group	Creates a Cisco Unified Communications Manager group and enters SCCP Cisco Unified Communications Manager configuration mode.
sccp local	Selects the local interface that SCCP applications use to register with Cisco Unified Communications Manager.

Command	Description
show sccp	Displays SCCP configuration information and current status.

sccp ccm group

To create a Cisco Unified Communications Manager group and enter SCCP Cisco CallManager configuration mode, use the **sccp ccm group** command in global configuration mode. To remove a particular Cisco Unified Communications Manager group, use the **no** form of this command.

sccp ccm group *group-number*
no sccp ccm group *group-number*

Syntax Description

group-number	Number that identifies the Cisco Unified Communications Manager group. Range is 1 to 50.

Command Default

No groups are defined, so all servers are configured individually.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.3(8)T	This command was introduced.
12.4(22)T	This command was modified. Support for IPv6 was added.
15.0(1)M	This command was modified. The group number range was increased to 50.

Usage Guidelines

Use this command to group Cisco Unified Communications Manager servers that are defined using the **sccp ccm** command. You can associate designated DSP farm profiles using the **associate profile** command so that the DSP services are controlled by the Cisco Unified Communications Manager servers in the group.

Examples

The following example enters SCCP Cisco CallManager configuration mode and associates Cisco Unified Communications Manager 25 with Cisco Unified Communications Manager group 10:

```
Router(config)#
sccp ccm group 10
Router(config-sccp-ccm)# associate ccm 25 priority 2
```

Related Commands

Command	Description
associate ccm	Associates a Cisco Unified Communications Manager server with a Cisco Unified Communications Manager group and establishes its priority within the group.
associate profile	Associates a DSP farm profile with a Cisco Unified Communications Manager group.
bind interface	Binds an interface with a Cisco Unified Communications Manager group.

Command	Description
connect interval	Specifies the amount of time that a DSP farm profile waits before attempting to connect to a Cisco Unified Communications Manager when the current Cisco Unified Communications Manager fails to connect.
connect retries	Specifies the number of times that a DSP farm attempts to connect to a Cisco Unified Communications Manager when the current Cisco Unified Communications Manager connections fails.
sccp ccm	Adds a Cisco Unified Communications Manager server to the list of available servers.

sccp codec mask

To mask a codec type so that it is not used by Cisco CallManager, use the **sccp codec mask**command in global configuration mode. To unmask a codec, use the **no** form of this command.

sccp codec *codec* **mask**
no sccp codec *codec* **mask**

Syntax Description

codec	Codec to mask. Values are the following: • **g711alaw** • **g711ulaw** • **g729abr8** • **g729ar8** • **g729br8** • **g729r8**

Command Default

No codecs are masked.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.1(5)YH4	This command was introduced.
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.
12.4(11)XJ2	The **gsmefr**and **gsmfr**keywords were removed as configurable codec options for all platforms with the exception of the **gsmfr** codec on the Cisco AS5400 and AS5350 with MSAv6 dsps.
12.4(15)T	This command was integrated into Cisco IOS Release 12.4(15)T.

Usage Guidelines

This command prevents the voice gateway from reporting codec types that are masked so that Cisco CallManager only selects codec types that are supported by the endpoints.

Note You must enable this command before Skinny Client Control Protocol (SCCP) is enabled. If the **sccp codec mask** command is used when SCCP is active, you must disable the SCCP using the **no sccp** command and then re-enable **sccp** for the **sccp codec mask** command to take effect.

Examples

The following example shows how to mask codec type G.711 ulaw and G.729r8:

```
sccp codec g711ulaw mask
sccp codec g729r8 mask
```

Related Commands

Command	Description
sccp	Enables SCCP and related applications.
sccp ccm	Adds a Cisco CallManager server to the list of available servers and sets various parameters.
sccp local	Selects the local interface that SCCP applications use to register with Cisco CallManager.
show sccp	Displays SCCP configuration information and current status.

sccp ip precedence

To set the IP precedence value to be used by Skinny Client Control Protocol (SCCP), use the **sccp ip precedence** command in global configuration mode. To reset to the default, use the **no** form of this command.

sccp ip precedence *value*
no sccp ip precedence

Syntax Description

value	IP precedence value. Range is from 1 (lowest) to 7 (highest).

Command Default

5

Command Modes

Global configuration (config)

Command History

Release	Modification
12.1(5)YH	This command was introduced on the Cisco VG200.
12.2(13)T	This command was implemented on the Cisco 2600 series, Cisco 3620, Cisco 3640, Cisco 3660, and Cisco 3700 series.
Cisco IOS XE Amsterdam 17.2.1r	Introduced support for YANG models.

Usage Guidelines

The router on which this command is used must be equipped with one or more digital T1/E1 packet voice trunk network modules (NM-HDVs) or high-density voice (HDV) transcoding/conferencing DSP farms (NM-HDV-FARMs) to provide digital-signal-processor (DSP) resources.

Examples

The following example sets IP precedence to the highest possible value:

```
Router# sccp ip precedence 1
```

Related Commands

Command	Description
dspfarm (DSP farm)	Enables DSP-farm service.
sccp	Enables SCCP and its associated transcoding and conferencing applications.
show sccp	Displays the SCCP configuration information and current status.

sccp local

To select the local interface that Skinny Client Control Protocol (SCCP) applications (transcoding and conferencing) use to register with Cisco CallManager, use the **sccp local** command in global configuration mode. To deselect the interface, use the **no** form of this command.

sccp local *interface-type interface-number* [**port** *port-number*]
no sccp local *interface-type interface-number*

Syntax Description

interface -type	Interface type that the SCCP application uses to register with Cisco CallManager. The type can be an interface address or a virtual-interface address such as Ethernet.
interface-number	Interface number that the SCCP application uses to register with Cisco CallManager.
port *port-number*	(Optional) Port number used by the selected interface. Range is 1025 to 65535. Default is 2000.

Command Default

No default behavior or values

Command Modes

Global configuration (config)

Command History

Release	Modification
12.1(5)YH	This command was introduced.
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.
12.3(14)T	The **port** keyword and *port-number* argument were added.

Usage Guidelines

The router must be equipped with one or more voice network modules that provide DSP resources.

Note If the default port is used by another application, the SCCP application fails to register to Cisco CallManager. Use the port keyword with the *port-number* argument to specify a different port for SCCP to use for registering with Cisco CallManager.

Examples

The following example selects a Fast Ethernet interface for SCCP applications to use to register with Cisco CallManager:

```
sccp local FastEthernet 0/0
```

Related Commands

Command	Description
dsp services dspfarm	Enables DSP-farm services.

Command	Description
sccp	Enables SCCP and its associated transcoding and conferencing applications.
show sccp	Displays the SCCP configuration information and current status.

sccp plar

To enter SCCP PLAR configuration mode, use the **sccp plar** command in global configuration mode. To disable private line automatic ringdown (PLAR) on all ports, use the **no** form of this command.

sccp plar
no sccp plar

Syntax Description

This command has no arguments or keywords.

Command Default

Disabled (PLAR is not enabled on any port).

Command Modes

Global configuration (config)

Command History

Release	Modification
12.4(6)T	This command was introduced.

Usage Guidelines

This command is used for enabling PLAR features on analog FXS endpoints that use Skinny Client Control Protocol (SCCP) for call control. Use the **voiceport** command to enable a specific analog voice port for PLAR.

Examples

The following example sets PLAR on voice ports 2/0, 2/1, and 2/3:

```
Router(config)# sccp plar
Router(config-sccp-plar)# voiceport 2/0 dial 3660 digit 1234 wait-connect 500 interval 200
Router(config-sccp-plar)# voiceport 2/1 dial 3264 digit 678,,,9*0,,#123 interval 100
Router(config-sccp-plar)# voiceport 2/3 dial 3478 digit 34567 wait-connect 500
```

Related Commands

Command	Description
dial peer voice	Enters dial-peer configuration mode and defines a dial peer.
voiceport	Enables a PLAR connection for an analog phone.

sccp switchback timeout guard

To set the Skinny Client Control Protocol (SCCP) switchback guard timer, use the **sccp switchback timeout guard** command in global configuration mode. To reset to the default, use the **no** form of this command.

sccp switchback timeout guard *seconds*
no sccp switchback timeout guard

Syntax Description

seconds	Guard timer value, in seconds. Range is from 180 to 7200. Default is 1200.

Command Default

1200 seconds

Command Modes

Global configuration (config)

Command History

Release	Modification
12.1(5)YH	This command was introduced on the Cisco VG200.
12.2(13)T	This command was implemented on the Cisco 2600 series, Cisco 3620, Cisco 3640, Cisco 3660, and Cisco 3700 series.

Usage Guidelines

The router on which this command is used must be equipped with one or more digital T1/E1 packet voice trunk network modules (NM-HDVs) or high-density voice (HDV) transcoding/conferencing DSP farms (NM-HDV-FARMs) to provide digital-signal-processor (DSP) resources.

You can use the guard timer value for the switchback algorithm that follows the Graceful Timer method.

Examples

The following example sets the switchback guard timer value to 180 seconds (3 minutes):

```
Router#
sccp switchback timeout guard 180
```

Related Commands

Command	Description
dspfarm (DSP farm)	Enables DSP-farm service.
sccp	Enables SCCP and its associated transcoding and conferencing applications.
show sccp	Displays the SCCP configuration information and current status.

scenario-cause

To configure new Q.850 call-disconnect cause codes for use if an H.323 call fails, use the **scenario-cause** command in H.323-voice-service configuration mode. To revert to the defaults, use the **no** form of this command.

scenario-cause {**arj-default** | **timeout** {**arq** | **t301** | **t303** | **t310**} *code-id*}
no scenario-cause {**arj-default** | **timeout** {**arq** | **t301** | **t303** | **t310**}}

Syntax Description

arj-default *code-id*	Q.850 call-disconnect cause code for use if a call fails for reasons that are assigned to the Admission Reject (ARJ) default cause code. Range: 1 to 127.
timeout arq *code-id*	Q.850 call-disconnect cause code for use if the H.323 gatekeeper Automatic Repeat Request (ARQ) timer expires. Range: 1 to 127.
timeout t301 *code-id*	Q.850 call-disconnect cause code for use when the H.225 alerting (T301) timer expires. Range: 1 to 127.
timeout t303 *code-id*	Q.850 call-disconnect cause code for use when the H.225 setup (T303) timer expires. Range: 1 to 127.
timeout t310 *code-id*	Q.850 call-disconnect cause code for use when the H.225 call-proceeding (T310) timer expires. Range: 1 to 127.

Command Default

No mapping occurs.

Command Modes

H.323 voice-service configuration (conf-serv-h323)

Command History

Release	Modification
12.4(9)T	This command was introduced.

Usage Guidelines

Use this command to configure new Q.850 call-disconnect cause codes for use if an H.323 voice call fails during setup.

Examples

The following example causes a gateway to send the default ARJ cause code of 24 rather than the previous default of 63 when a call fails for reasons that are associated with the ARJ default cause code:

```
Router(config)# voice service voip
Router(conf-voi-serv)# h323
Router(conf-serv-h323)# scenario-cause arj-default 24
```

Related Commands

Command	Description
h225 timeout call-proceeding	Sets the call-proceeding (T310, or call-setup to call-disconnect) disconnect timer.

Command	Description
map q850-cause	Maps a Q.850 call-disconnect cause code to a tone.
q850-cause	Maps a Q.850 call-disconnect cause code to a different Q.850 call-disconnect cause code.

sdspfarm tag

To permit a digital-signal-processor (DSP) farm to be to registered to Cisco Unified CME and associate it with the MAC address of a Skinny Client Control Protocol (SCCP) interface, use the **sdspfarm tag** command in telephony-service configuration mode. To delete a tag generated by the **sdspfarm tag**command, use the **no** form of this command.

sdspfarm tag *number device-name*
no sdspfarm tag *number device-name*

Syntax Description

number	Numeric name for a DSP farm. Number from 1 to 10.
device-name	Word describing the device, such as the MAC address, of the SCCP client interface that is preceded by the Message Transfer Part (MTP).

Command Default

DSP farm is not created.

Command Modes

Telephony-service configuration (config-telephony)

Command History

Cisco IOS Release	Cisco Product	Modification
12.3(11)T	Cisco CME 3.2	This command was introduced.
15.1(4)M	Cisco CME 8.6	This command was modified. The maximum number used to tag a DSP farm was increased to 10.

Usage Guidelines

DSP farm profiles are sets of DSP resources used for conferencing and transcoding only. DSP farms do not include voice termination resources. Use the **show interface**command to find the MAC address of the SCCP client interface.

Examples

The following example declares tag 1 as the MAC address of mac000a.8aea.ca80. The **show interface** command is used to obtain the MAC address.

```
Router#
show interface FastEthernet 0/0
.
.
.
FastEthernet0/0 is up, line protocol is up
Hardware is AmdFE, address is 000a.8aea.ca80 (bia 000a.8aea.ca80)
.
.
.
Router(config)# telephony-service
Router(config-telephony)# sdspfarm tag 1 mac000a.8aea.ca80
```

Related Commands

Command	Description
sdspfarm transcode	Specifies the maximum number of transcoding sessions allowed per Cisco CME router.
sdspfarm units	Specifies the maximum number of DSP farms that are allowed to be registered to the SCCP server.

sdspfarm transcode sessions

To specify the maximum number of transcoding sessions allowed per Cisco CallManager Express (Cisco CME) router, use the **sdspfarm transcode sessions**command in telephony-service configuration mode. To return to the default transcode session of 0, use the **no** form of this command.

sdspfarm transcode sessions *number*
no sdspfarm transcode sessions *number*

Syntax Description

number	Declares the number of DSP farm sessions. Valid values are numbers from 1 to 128.

Command Default

The default is 0.

Command Modes

Telephony-service configuration (config-telephony)

Command History

Cisco IOS Release	Cisco Product	Modification
12.3(11)T	Cisco CME 3.2	This command was introduced.

Usage Guidelines

The transcoding is allowed between G.711 and G.729. A session consists of two transcode streams. To configure this information, you must know how many digital-signal-processor (DSP) farms are configured on the network module (NM) farms in your Cisco CME router. DSP farms are sets of DSP resources used for conferencing and transcoding only. DSP farms do not include voice termination resources. To learn how many DSP farms have been configured on your Cisco CME router, use the **show sdspfarm** command.

Examples

The following example sets the maximum number of transcoding sessions allowed on the Cisco CME router to 20:

```
Router(config)# telephony-service

Router(config-telephony)# sdspfarm transcode sessions 20
```

Related Commands

Command	Description
sdspfarm tag	Declares a DSP farm and associates it with an SCCP client interface's MAC address.
sdspfarm unit	Specifies the maximum number of DSP farms that are allowed to be registered to the SCCP server.
show sdspfarm	Displays the status of the configured DSP farms and transcoding streams.

sdspfarm units

To specify the maximum number of digital-signal-processor (DSP) farm profiles that are allowed to be registered to the Skinny Client Control Protocol (SCCP) server, use the **sdspfarm units** command in telephony-service configuration mode. To set the number of DSP farm profiles to the default value of 0, use the **no** form of this command.

sdspfarm units *number*
no sdspfarm units *number*

Syntax Description

number	Number of DSP farms. Valid values are numbers from 0 to 10.

Command Default

The default number is 0.

Command Modes

Telephony-service configuration (config-telephony)

Command History

Cisco IOS Release	Cisco Product	Modification
12.3(11)T	Cisco CME 3.2	This command was introduced.
15.1(4)M	Cisco CME 8.6	This command was modified. The command increased support for the maximum number of DSP farms to 10.

Usage Guidelines

DSP farm profiles are sets of DSP resources used for conferencing and transcoding only. DSP farm profiles do not include voice termination resources.

Examples

The following example configures a Cisco CME router to register one DSP farm:

```
Router(config)# telephony-service
Router(config-telephony)# sdspfarm units 1
```

Related Commands

Command	Description
sdspfarm tag	Declares a DSP farm and associates it with the MAC address of an SCCP client interface.
sdspfarm transcode	Specifies the maximum number of transcoding sessions allowed per Cisco CME router.

secondary

To set the backup location for storing call detail records (CDRs) if the primary location becomes unavailable, use the **secondary** command in gateway accounting file configuration mode. To reset to the default, use the **no** form of this command.

secondary { **ftp** *path/filename* **username** *username* **password** { **<0-7>** | **LINE** } *password* | **ifs** *device* **:** *filename* | **sftp** *<server>[:<port>]/<path>* **username** *username* **password** { **0** | **6** } *password* }
no secondary { **ftp** | **ifs** | **sftp** }

Syntax Description

ftp *path /filename*	Name and location of the backup file on an external FTP server. Filename is limited to 25 characters.
ifs *device* **:** *filename*	Name and location of the backup file in flash memory or other internal file system on this router. Values depend on storage devices available on the router, for example flash or slot0. Filename is limited to 25 characters.
sftp *<server>[:<port>]/<path>*	Specifies the SFTP mode of file transfer
password {*0* | *6* } **password** {*<0-7 >*| *LINE* }	Following are the password encryption types– • **0**– Specifies that the subsequent password is in plain text. Type **0** disables encryption. • **6**– Specifies that the subsequent password is encrypted using the AES algorithm. Ensure to provide a string in AES-encrypted format. • **7**– Specifies that the subsequent password is hidden. You must enter a Cisco-proprietary encrypted password string. • **LINE**– The cleartext password.
username *username*	User ID for authentication.
password *password*	Password user enters for authentication.

Command Default

Call records are saved to **flash:cdr**.

Command Modes

Gateway accounting file configuration (config-gw-accounting-file)

Command History

Release	Modification
Cisco IOS XE 26.2.1	This command was modified for the following: • To support Type 6 encryption. • To display warning message for insecure protocol usage.
12.4(20)T	This command was integrated into Cisco IOS Release 12.4(20)T.
12.4(15)XY	This command was introduced.

Usage Guidelines

This command defines the backup location where accounting records are sent if the file transfer to the primary device fails. The file accounting process retries the primary device, defined with the **primary** command, up to the number of times defined by the **maximum retry-count** command before automatically switching over to the secondary device.

The secondary device is attempted only after the primary device fails after the defined number of retries. If the secondary device also fails, the system logs an error and the file accounting process stops.

To manually switch back to the primary device when it becomes available, use the **file-acct reset** command. The system does not automatically switch back to the primary device.

A syslog warning message is generated if flash becomes full.

The filename you assign is appended with the gateway hostname and time stamp at the time the file is created to make the filename unique. For example, if you specify the filename cdrtest1 on a router with the hostname cme-2821, a file is created with the name cdrtest1.cme-2821.2007_10_28T22_21_41.000, where 2007_10_28T22_21_41.000 is the time that the file was created.

Limit the filename you assign with this command to 25 characters, otherwise it could be truncated when the accounting file is created because the full filename, including the appended hostname and timestamp, is limited to 63 characters.

Starting from Cisco IOS XE 26.2.1 release, it is recommended to use Type 6 (AES) for all credential provisioning to comply with security standards. Usage of Type 0, or 7 triggers a syslog warning. Ensure **password encryption aes** and **key config-key password-encrypt** are enabled to support auto-conversion of Type 0, or 7 to Type 6 reversible encryption. If the encryption commands are not enabled, 0 and 7 password types are not converted to type 6; they remain saved as type 0 and 7.



Warning Starting with Cisco IOS XE 26.2.1, a warning message is displayed when insecure protocols such as HTTP, FTP, or TFTP are used, as they do not provide encryption or authentication. Use secure alternatives such as HTTPS, SFTP, or SCP instead.

Examples

The following example shows how to configure external SFTP server with unencrypted type of password:

```
Device(config)#gw-accounting file
Device(config-gw-accounting-file)#secondary sftp sftp://john:doe@abc:23//directory1/directory2

username myname password 0 password
```

The following example shows the warning message being displayed for the usage of insecure FTP protocol:

```
Device(config)#gw-accounting file
Device(config-gw-accounting-file)#secondary ftp server1/cdrtest1 username myname password
0 password
SECURITY WARNING - Module: GATEWAY_ACCOUNTING, Command: secondary ftp server1/cdrtest1
username myname password 0 *,
Reason: No encryption is configured, Description: Gateway accounting primary file transfer
 configured with insecure FTP protocol -
vulnerable to credential theft,
Remediation: Transition to secure file transfer methods using SCP, SFTP, HTTPS protocols
```

The following example enables type 6 auto-conversion:

```
Router(config)# password encryption aes
Router(config)# key config-key password-encrypt
Old Key:
New Key :
Confirm Key :
Router(config)# gw-accounting file
Router(config-gw-accounting-file)# secondary sftp
sftp://john:doe@abc:23//directory1/directory2 username myname password 0 password
Router(config-gw-accounting-file)# end

Router#do sh run | sec gw-accou
primary sftp sftp://john:doe@abc:23//directory1/directory2 username myname password 6
EMSefGVigEAMP][YVUF\ZPDbCD^PJQ
```

The following example shows the backup location of the accounting file is set to flash:cdrtest2:

```
gw-accounting file
 primary ftp server1/cdrtest1 username bob password temp
 secondary ifs flash:cdrtest2
 maximum buffer-size  25
 maximum retry-count 3
 maximum fileclose-timer 720
 cdr-format compact
```

Related Commands

Command	Description
file-acct reset	Manually switches back to the primary device for file accounting.
maximum retry-count	Sets the maximum number of times the router attempts to connect to the primary file device before switching to the secondary device.
primary	Sets the primary location for storing the CDRs generated for file accounting.

secure-ciphersuite

To configure the cipher suites (encryption algorithms) to be used for encryption over HTTPS for a WebSocket connection in CUBE, use the **secure-ciphersuite** command in media profile stream-service configuration mode. To revert to the command default, use the **no** form of this command.

secure-ciphersuite *list*
no secure-ciphersuite *list*

Syntax Description

list	List of cipher suites supported with the WebSockets in CUBE. Starting from Cisco IOS XE Dublin 17.12.1a, CUBE supports GCM cipher in addition to the other supported ciphers. The following list of cipher suites are supported for WebSocket connections: • aes-128-cbc-sha • dhe-rsa-aes-cbc-sha2 • ecdhe-rsa-aes-cbc-sha2 • rsa-aes-cbc-sha2 • ecdhe-ecdsa-aes-gcm-sha2 • ecdhe-rsa-aes-gcm-sha2

Command Default

By default, all cipher suites including GCM cipher suites are supported for WebSocket connections.

Command Modes

Media Profile Stream-Service configuration mode (cfg-mediaprofile)

Command History

Release	Modification
Cisco IOS XE Bengaluru 17.6.1a	This command was introduced on CUBE.
Cisco IOS XE Dublin 17.12.1a	Added support for GCM cipher negotiation for WebSocket based media forking.

Usage Guidelines

Use the **secure-ciphersuite** command to configure the cipher suites (encryption algorithms) for encryption over HTTPS for a WebSocket connection in CUBE.

Configure **no secure-ciphersuite** to enable the default behavior. However, you can limit negotiation to a selected set of one or more cipher suites using **secure-ciphersuite** *list* command.

Starting from Cisco IOS XE Dublin 17.12.1a, CUBE supports GCM cipher suites for WebSocket connections in addition to the other supported ciphers.

Examples

The following example shows how to configure secure ciphers for WebSockets in CUBE:

```
Device(config)#media profile stream-service 1
```

```
Device(cfg-mediaprofile)#secure-ciphersuite ?
  aes-128-cbc-sha           Encryption tls_with_aes-128-cbc-sha2 ciphersuite
  dhe-rsa-aes-cbc-sha2      Encryption tls_rsa_with_cbc_sha2 ciphersuite
  ecdhe-rsa-aes-cbc-sha2    Encryption tls_rsa_with_aes-cbd-sha2 ciphersuite
  rsa-aes-cbc-sha2          Encryption tls_rsa_with_aes_cbc_sha2 ciphersuite
  ecdhe-ecdsa-aes-gcm-sha2  Encryption tls_rsa_with_ecdhe-ecdsa-aes-gcm-sha2 ciphersuite
  ecdhe-rsa-aes-gcm-sha2    Encryption tls_rsa_with_aes-gcm-sha2 ciphersuite
Device(cfg-mediaprofile)#secure-ciphersuite tls_rsa_with_cbc_sha2
  WS Client Secure Ciphersuite: tls_rsa_with_cbc_sha2
Device(cfg-mediaprofile)#
```

Related Commands

Command	Description
media profile stream-service	Enables stream service on CUBE.
connection (media-profile)	Configures idle timeout and call threshold for a media profile.
proxy (media-profile)	Configures IP address or hostname of proxy in the media profile configuration mode.
description (media-profile)	Specifies a description for the media profile.
media class	Applies the media class at the dial peer level.

security

To enable authentication and authorization on a gatekeeper, use the **security** command in gatekeeper configuration mode. To disable security, use the **no** form of this command.

security {**any** | **h323-id** | **e164**} {**password default** *password* | **password separator** *character*}
no security {**any** | **h323-id** | **e164**} {**password default** *password* | **password separator** *character*}

Syntax Description

any	Uses the first alias of an incoming registration, admission, and status (RAS) protocol registration, regardless of its type, to identify the user to RADIUS/TACACS+.
h323 -id	Uses the first H.323 ID type alias to identify the user to RADIUS/TACACS+.
e164	Uses the first E.164 address type alias to identify the user to RADIUS/TACACS+.
password default *password*	Default password that the gatekeeper associates with endpoints when authenticating them with an authentication server. The password must be identical to the password on the authentication server.
password separator *character*	Character that endpoints use to separate the H.323-ID from the piggybacked password in the registration. Specifying this character allows each endpoint to supply a user-specific password. The separator character and password are stripped from the string before it is treated as an H.323-ID alias to be registered. Note that passwords may only be piggybacked in the H.323-ID, not the E.164 address, because the E.164 address allows a limited set of mostly numeric characters. If the endpoint does not wish to register an H.323-ID, it can still supply an H.323-ID consisting of just the separator character and password. This H.323-ID consisting of just the separator character and password are understood to be a password mechanism and no H.323-ID is registered.

Command Default

No default

Command Modes

Gatekeeper configuration (config-gk)

Command History

Release	Modification
11.3(2)NA	This command was introduced on the Cisco 2600 series and Cisco 3600 series.

Usage Guidelines

Use this command to enable identification of registered aliases by RADIUS/TACACS+. If the alias does not exist in RADIUS/TACACS+, the endpoint is not allowed to register.

A RADIUS/TACACS+ server and encryption key must have been configured in Cisco IOS software for security to work.

Only the first alias of the proper type is identified. If no alias of the proper type is found, the registration is rejected.

This command does not allow you to define the password mechanism unless the security type (**h323-id** or **e164** or **any**) has been defined. Although the **no security password** command undefines the password

mechanism, it leaves the security type unchanged, so security is still enabled. However, the **no security** command disables security entirely, including removing any existing password definitions.

Examples

The following example enables identification of registrations using the first H.323 ID found in any registration:

```
security h323id
```

The following example enables security, authenticating all users by using their H.323-IDs and a password of qwerty2x:

```
security h323-id
security password qwerty2x
```

The next example enables security, authenticating all users by using their H.323-IDs and the password entered by the user in the H.323-ID alias he or she registers:

```
security h323-id
security password separator !
```

If a user registers with an H.323-ID of joe!024aqx, the gatekeeper authenticates user joe with password 024aqx, and if that is successful, registers the user with the H.323-ID of joe. If the exclamation point is not found, the user is authenticated with the default password, or a null password if no default has been configured.

The following example enables security, authenticating all users by using their E.164 IDs and the password entered by the user in the H.323-ID alias he or she registers:

```
security e164
security password separator !
```

If a user registers with an E.164 address of 5551212 and an H.323-ID of !hs8473q6, the gatekeeper authenticates user 5551212 and password hs8473q6. Because the H.323-ID string supplied by the user begins with the separator character, no H.323-ID is registered, and the user is known only by the E.164 address.

Related Commands

Command	Description
accounting (gatekeeper)	Enables the accounting security feature on the gatekeeper.
radius-server host	Specifies a RADIUS server host.
radius -server key	Sets the authentication and encryption key for all RADIUS communications between the router and the RADIUS daemon.

security acl

To configure access-list based filtering on the gatekeeper, use the **security acl**command in gatekeeper configuration mode. To disable, use the no form of this command.

security acl {**answerarq** | **lrq**} *access-list-number*
no security acl {**answerarq** | **lrq**}

Syntax Description

answerarq	Filters incoming answer admission requests (AnswerARQ) using IP access-lists.
lrq	Filters incoming location requests (LRQs) using IP access-list.
access-list-number	Number of an access list that was configured using the access-list command. This is a decimal number from 1 to 99 or from 1300 to 1999. Only standard IP access lists numbered 1 through 99 are supported for the Tokenless Call Authorization feature.

Command Default

No default behavior or values.

Command Modes

Gatekeeper configuration (config-gk)

Command History

Release	Modification
12.3(5)	This command was introduced.

Usage Guidelines

The **security acl** command configures the gatekeeper to use IP access lists for security. Use this command in conjunction with the **access-list** command to configure access-list based AnswerARQ and LRQ requests filtering on a gatekeeper. The gatekeeper will process only those requestswhich have been sent by sources that are permitted access by the specified IP access list. Requests sent by sources which have been denied by the specified IP access lists, will be rejected.

Examples

The following example shows how to configure a gatekeeper to use a previously configured IP access list with an IP access list number of 30 for call authorization:

```
Router(config-gk)# security acl answerarq 30
```

The following example shows how to configure a gatekeeper to use a previously configured IP access list with an IP access list number of 20 for LRQ filtering:

```
Router(config-gk)# security acl lrq 20
```

Related Commands

Command	Description
access -list	Configures the access list mechanism for filtering frames by protocol type or vendor code.

security izct

To configure the gatekeeper to include the destination E.164 alias in the IZC token hash, use the **security izct** command in gatekeeper configuration mode. To not include destination E.16 alias in IZC token hash, use the **no** form of this command.

security izct password *password* [**hash** {**dest-alias** | **src-alias** | **dest-csa** | **src-csa** | **dest-epid** | **src-epid**}]
no security izct *password* [**hash** {**dest-alias** | **src-alias** | **dest-csa** | **src-csa** | **dest-epid** | **src-epid**}]

Syntax Description

password *password*	Specifies the password that the gatekeeper associates with endpoints when authenticating them with an authentication server. The password must be identical to the password on the authentication server.
hash	Specifies the options to be used in hash generation.
dest-alias	Specifies that the destination alias be included in hash generation.
src-alias	Specifies that the source alias be included in hash generation.
dest-csa	Specifies that the destination csa be included in hash generation.
src-csa	Specifies that the source alias be included in hash generation.
dest-epid	Specifies that the destination epid be included in hash generation.
src-epid	Specifies that the source epid be included in hash generation.

Command Default

Destination E.16 alias are not included in IZC token hash.

Command Modes

Gatekeeper configuration (config-gk)

Command History

Release	Modification
12.3(5)	This command was introduced.
12.4(15)XZ	The **dest-alias, src-alias, dest-csa, src-csa, dest-epid,**and **src-epid**keywords were added.
12.4(20)T	This command was integrated into Cisco IOS Release 12.4(20)T.

Usage Guidelines

Configure the **security izct** command on the gatekeeper that generates the InterZone Clear Token (IZCT) hash to prevent rogue endpoints from sending an ARQ message with one called number and then changing the called number when they send the SETUP message to the terminating endpoint. When this command is configured, modification of the called number after the IZCT hash is generated by the trunking gateway will not be allowed. The IZCT token generated is valid only for 30 seconds and the IZCT hash token generated by terminating gatekeeper (TGK) can be used for multiple calls.

The call is rejected if any intermediate entity, such as a Cisco Gatekeeper Transaction Message Protocol (GKTMP) server (on the originating gatekeeper) or the originating gateway (using number translation rules), tries to modify the called number after the token is prepared during address resolution.

- The **hash** keyword at originating gateway (OGW) and TGK do not need to match.
- More than one **hash** keyword can be configured for the **security izct**command.

The **security izct**command must be configured at OGK or TGK in order to enable the feature.

When configuring an OGW to an OGK to a TGK and to a TGW. The **security izct**command is optional at the OGK, and required at the TGK. If hash parameter is not specified at the TGK, then dest-alias (default) will be used for hash token computation.

The **no** version of this command the requires the keyword argument combinations as defined in the preceding command syntax table.

Examples

The following example prevents modification of the called number after the IZCT hash is generated by the trunking gateway:

```
Router(config-gk)# security izct password example hash dest-alias
```

Related Commands

Command	Description
accounting (gatekeeper)	Enables the accounting security feature on the gatekeeper.
radius-server host	Specifies a RADIUS server host.
radius-server key	Sets the authentication and encryption key for all RADIUS communications between the router and the RADIUS daemon.

security mode

To set the security mode for a specific dial peer using Skinny Client Control Protocol (SCCP) Telephony Control Application (STCAPP) services in a secure Cisco Unified CME network, use the **security mode** command in dial peer configuration mode. To return to the default, use the **no** form of this command.

security mode {**authenticated** | **none** | **encrypted** | **system**}
no security mode

Syntax Description

authenticated	Sets the security mode to authenticated and enables SCCP signaling between the voice gateway and Cisco Unified CME to take place through the secure TLS connection on TCP port 2443.
none	SCCP signaling is not secure.
encrypted	Sets the security mode to encrypted and enables SCCP signaling between the voice gateway and Cisco Unified CME to take place through Secure Real-Time Transport Protocol (SRTP).
system	Enables the security mode specified at the global level by the **stcapp security mode** command.

Command Default

Security mode specified at the global level is enabled.

Command Modes

Dial peer configuration (config-dialpeer)

Command History

Release	Modification
12.4(11)XW1	This command was introduced.
12.4(20)T	This command was integrated into Cisco IOS Release 12.4(20)T.

Usage Guidelines

Use this command to specify security mode on the voice gateway for Cisco Unified CME phone authentication and encryption.

Set the SCCP signaling security mode globally using the **stcapp security mode** command in global configuration mode. If you use both the **stcapp security mode** and the **security mode**commands, the dial-peer level command, **security mode**, overrides the global setting.

Examples

The following example selects secure SCCP signaling in authenticated mode:

```
Router(config)# dial-peer voice 1 pots
Router(config-dialpeer)# security mode authenticated
```

The following example selects encrypted secure SCCP signaling and encryption through SRTP:

```
Router(config)# dial-peer voice 2 pots
Router(config-dialpeer)# security mode encrypted
```

Related Commands

Command	Description
stcapp security mode	Enables security for STCAPP endpoints and specifies the security mode to be used for setting up the TLS connection.

sequence-numbers

To enable the generation of sequence numbers in each frame generated by the digital signal processor (DSP) for Voice over Frame Relay applications, use the **sequence-numbers** command in dial-peer configuration mode. To disable the generation of sequence numbers, use the **no** form of this command.

sequence-numbers
no sequence-numbers

Syntax Description

This command has no arguments or keywords.

Command Default

Disabled

Command Modes

Dial peer configuration (config-dial-peer)

Command History

Release	Modification
12.0(3)XG	This command was introduced on the Cisco 2600 series, Cisco 3600 series, and Cisco MC3810.
12.0(4)T	This command was integrated into Cisco IOS Release 12.0(4)T.

Usage Guidelines

Sequence numbers on voice packets allow the digital signal processor (DSP) at the playout side to detect lost packets, duplicate packets, or out-of-sequence packets. This helps the DSP to mask out occasional drop-outs in voice transmission at the cost of one extra byte per packet. The benefit of using sequence numbers versus the cost in bandwidth of adding an extra byte to each voice packet on the Frame Relay network must be weighed to determine whether to disable this function for your application.

Another factor to consider is that this command does not affect codecs that require a sequence number, such as G.726. If you are using a codec that requires a sequence number, the DSP generates one regardless of the configuration of this command.

Examples

The following example disables generation of sequence numbers for VoFR frames for VoFR dial peer 200:

```
dial-peer voice 200 vofr
 no sequence-numbers
```

Related Commands

Command	Description
called -number (dial-peer)	Enables an incoming VoFR call leg to get bridged to the correct POTS call leg when using a static FRF.11 trunk connection.
codec (dial -peer)	Specifies the voice coder rate of speech for a Voice over Frame Relay dial peer.
cptone	Specifies a regional analog voice interface-related tone, ring, and cadence setting.

Command	Description
destination -pattern	Specifies either the prefix, the full E.164 telephone number, or an ISDN directory number (depending on the dial plan) to be used for a dial peer.
dtmf -relay (Voice over Frame Relay)	Enables the generation of FRF.11 Annex A frames for a dial peer.
session protocol (Voice over Frame Relay)	Establishes a session protocol for calls between the local and remote routers via the packet network.
session target	Specifies a network-specific address for a specified dial peer or destination gatekeeper.
signal -type	Sets the signaling type to be used when connecting to a dial peer.

server (auto-config application)

To configure the IP address or name of the TFTP server for an auto-configuration application, use the **server** command in auto-config application configuration mode. To remove the IP address or name, use the **no** form of this command.

{**server** *ip-address* | *domain-name* [*ip-addressdomain-name*] [*ip-addressdomain-name*]}
no server

Syntax Description

ip-address	Specifies the IP address of the TFTP server.
domain-name	Specifies the domain name of the TFTP server.

Command Default

No default behavior or values.

Command Modes

Auto-config application configuration (auto-config-app)

Command History

Release	Modification
12.3(8)XY	This command was introduced on the Communication Media Module.
12.3(14)T	This command was integrated into Cisco IOS Release 12.3(14)T.

Examples

The following example shows the **server** command used to configure two TFTP servers for an auto-configuration application:

```
Router(auto-config-app)# server 172.18.240.45 172.18.240.55
```

Related Commands

Command	Description
auto-config	Enables auto-configuration or enters auto-config application configuration mode for the Skinny Client Control Protocol (SCCP) application.
show auto-config	Displays the current status of auto-config applications.

server (presence)

To specify the IP address of a presence server for sending presence requests from internal watchers to external presence entities, use the **server**command in presence configuration mode. To remove the server, use the **no** form of this command.

server *ip-address*
no server

Syntax Description

ip-address	IP address of the remote presence server.

Command Default

A remote presence server is not used.

Command Modes

Presence configuration (config-presence)

Command History

Release	Modification
12.4(11)XJ	This command was introduced.
12.4(15)T	This command was integrated into Cisco IOS Release 12.4(15)T.

Usage Guidelines

This command specifies the IP address of a presence server that handles presence requests when the watcher and presence entity (presentity) are not collocated. The router acts as the presence server and processes all presence requests and status notifications when a watcher and presentity are both internal. If a subscription request is for an external presentity, the request is sent to the remote server specified by this command.

Examples

The following example shows a presence server with IP address 10.10.10.1:

```
Router(config)# presence
Router(config-presence)# allow subscribe
Router(config-presence)# server 10.10.10.1
```

Related Commands

Command	Description
allow subscribe	Allows internal watchers to monitor external presence entities (directory numbers).
allow watch	Allows a directory number on a phone registered to Cisco Unified CME to be watched in a presence service.
max-subscription	Sets the maximum number of concurrent watch sessions that are allowed.
show presence global	Displays configuration information about the presence service.
show presence subscription	Displays information about active presence subscriptions.

Command	Description
watcher all	Allows external watchers to monitor internal presence entities (directory numbers).

server (RLM)

To identify an RLM server, use the **server** RLM configuration command. To remove the identification, use the **no** form of this command

server *name-tag*
no server *name-tag*

Syntax Description

name -tag	Name to identify the server configuration so that multiple entries of server configuration can be entered.

Command Default

Disabled

Command Modes

RLM configuration

Command History

Release	Modification
11.3(7)	This command was introduced.

Usage Guidelines

Each server can have multiple entries of IP addresses or aliases.

Examples

The following example identifies the RLM server and defines the associated IP addresses:

```
rlm group 1
 server rl-server
 link address 10.1.4.1 source Loopback1 weight 4
 link address 10.1.4.2 source Loopback2 weight 3
```

Related Commands

Command	Description
clear interface	Resets the hardware logic on an interface.
clear rlm group	Clears all RLM group time stamps to zero.
interface	Defines the IP addresses of the server, configures an interface type, and enters interface configuration mode.
link (RLM)	Specifies the link preference.
protocol rlm port	Reconfigures the port number for the basic RLM connection for the whole rlm-group.
retry keepalive	Allows consecutive keepalive failures a certain amount of time before the link is declared down.
show rlm group statistics	Displays the network latency of the RLM group.
show rlm group status	Displays the status of the RLM group.

Command	Description
show rlm group timer	Displays the current RLM group timer values.
shutdown (RLM)	Shuts down all of the links under the RLM group.
timer	Overwrites the default setting of timeout values.

server absent reject

To configure the gatekeeper to reject new registrations or calls when the connection to the Gatekeeper Transaction Message Protocol (GKTMP) server is down, use the **server absent reject** command in gatekeeper configuration mode. To disable, use the no form of this command.

server absent reject {**arq** | **rrq**}
no server absent reject {**arq** | **rrq**}

Syntax Description

arq	Reject call admission request (ARQ) messages.
rrq	Reject registration request (RRQ) messages.

Command Default

By default, registrations and calls are not rejected.

Command Modes

Gatekeeper configuration (config-gk)

Command History

Release	Modification
12.2(11)T	This command was introduced on the Cisco 3660 and Cisco MC3810.

Usage Guidelines

This command configures the gatekeeper to reject new registrations or calls when it is unable to reach the GKTMP server because the TCP connection between the gatekeeper and GKTMP server is down. If multiple GKTMP servers are configured, the gatekeeper tries all of them and rejects registrations or calls only if none of the servers respond. You can also use this feature for security or service denial if a connection with the server is required to complete a registration.



Note This command assumes that RRQ and ARQ triggers are used between the gatekeeper and GKTMP server.

Examples

The following example directs the gatekeeper to reject registrations when it cannot connect to the GKTMP server:

```
Router# show gatekeeper configuration
.
.
.
h323id tet
 gw-type-prefix 1#* default-technology
 gw-type-prefix 9#* gw ipaddr 1.1.1.1 1720
 no shutdown
 server absent reject rrq
.
.
.
```

server flow-control

To enable flow control on the Cisco IOS gatekeeper (GK) and reset all thresholds to default, use the **server flow-control** command in gatekeeper configuration mode. To disable GK flow control, use the **no** form of this command.

server flow-control [**onset** *value*] [**abatement** *value*] [**qcount** *value*]
no server flow-control

Syntax Description

onset *value*	(Optional) Percentage of the server timeout value that is used to mark the server as usable or unusable. Range is from 1 to 100. The default is 80.
abatement *value*	(Optional) Percentage of the server timeout value that is used to mark the server as unusable or usable. Range is from 1 to 100. The default is 50. **Note** The abatement value must be less than the onset value.
qcount *value*	(Optional) Threshold length of the outbound queue on the GK. The queue contains messages waiting to be transmitted to the server. The TCP socket between the GK and Gatekeeper Transaction Message Protocol (GKTMP) server queues messages if it has too many to transmit. If the count of outbound queue length on the server reaches the qcount value, the server is marked unusable. Range is from 1 to 1000. The default is 400.

Command Default

The gatekeeper will send a maximum of 1000 RRQ messages.

Command Modes

Gatekeeper configuration (config-gk)

Command History

Release	Modification
12.2(2)XB	This command was introduced.
12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T.

Usage Guidelines

Suppose the server timeout value is 3 seconds, the onset value is 50, and the abatement value is 40. When the average response time from the server to the Gatekeeper Transaction Message Protocol (GKTMP) reaches 1.5 seconds (the onset percentage of the server timeout value), the server is marked as unusable. During the period that the server is marked as unusable, REQUEST ALV messages are still sent to the unusable server. When the response time is lowered to 1.2 seconds (the abatement percentage of the timeout value), the server is marked usable again, and the GKTMP resumes sending messages to the server.

When the **server flow-control** command is configured on its own the default is value 400. If you change one parameter using the **server flow-control** command, all other parameters revert to the default values. For example, if the onset is configured at 70 percent and you use the **server flow-control**command to set the abatement level, the onset resets to the default (80 percent).

Examples

The following example uses the command with the default values:

```
Router# server flow-control
```

The following example enables the GKTMP Interface Resiliency Enhancement feature with an onset level of 50:

```
Router# server flow-control onset 50
*Mar  8 20:05:34.081: gk_srv_handle_flowcontrol: Flow control enabled
Router# show running-config
Building configuration...
Current configuration : 1065 bytes
!
version 12.2
no service single-slot-reload-enable
service timestamps debug datetime msec
service timestamps log uptime
no service password-encryption
!
hostname snet-3660-3
!
.
.
.
gatekeeper
 zone local snet-3660-3 cisco.com
 zone remote snet-3660-2 cisco.com 209.165.200.225 1719
 zone prefix snet-3660-2 408*
 lrq forward-queries
 no use-proxy snet-3660-3 default inbound-to terminal
 no use-proxy snet-3660-3 default outbound-from terminal
 no shutdown
 server registration-port 8000
 server flow-control onset 50
!
.
.
.
end
```

The following example enables the GKTMP Interface Resiliency Enhancement feature:

```
Router# show gatekeeper status
Gatekeeper State: UP
    Load Balancing:   DISABLED
    Flow Control:     ENABLED
    Zone Name:        snet-3660-3
    Accounting:       DISABLED
    Endpoint Throttling:        DISABLED
    Security:         DISABLED
    Maximum Remote Bandwidth:              unlimited
    Current Remote Bandwidth:              0 kbps
    Current Remote Bandwidth (w/ Alt GKs): 0 kbps
```

The following example shows the server statistics, including timeout encountered, average response time, and the server status:

```
Router# show gatekeeper server
            GATEKEEPER SERVERS STATUS
            =========================
Gatekeeper Server listening port: 8250
Gatekeeper Server timeout value: 30 (100ms)
GateKeeper GKTMP version: 3.1
```

```
Gatekeeper-ID: Gatekeeper1
------------------------
  RRQ  Priority: 5
    Server-ID: Server43
    Server IP address: 209.165.200.254:40118
    Server type: dynamically registered
    Connection Status: active
    Trigger Information:
      Trigger unconditionally
    Server Statistics:
    REQUEST RRQ Sent=0
    RESPONSE RRQ Received = 0
    RESPONSE RCF Received = 0
    RESPONSE RRJ Received = 0
    Timeout encountered=0
    Average response time(ms)=0
    Server Usable=TRUE
```

Related Commands

Command	Description
timer server timeout	Specifies the timeout value for a response from a back-end GKTMP server.

server registration-port

To configure the listener port for the server to establish a connection with the gatekeeper, use the **server registration-port** command in gatekeeper configuration mode. To force the gatekeeper to close the listening socket so that no more new registration takes place, use the **no** form of this command.

server registration-port *port-number*
no server registration-port *port-number*

Syntax Description

port -number	Port number on which the gatekeeper listens for external server connections. Range is from 1 to 65535. There is no default.

Command Default

No registration port is configured.

Note If the gatekeeper is to communicate with network servers, a registration port must be configured on it.

Command Modes

Gatekeeper configuration (config-gk)

Command History

Release	Modification
12.1(1)T	This command was introduced on the following platforms: Cisco 2500 series, Cisco 2600 series, Cisco 3600 series, Cisco 7200 series, and Cisco MC3810.
12.2(11)T	This command was implemented on the Cisco 3700 series.

Usage Guidelines

Use this command to configure a server registration port to poll for servers that want to establish connections with the gatekeeper.

Note The no form of this command forces the gatekeeper on this router to close the listen socket, so it cannot accept more registrations. However, existing connections between the gatekeeper and servers are left open.

Examples

The following example establishes a listener port for a server connection with a gatekeeper:

```
Router(config)# gatekeeper
Router(config-gk)# server registration-port 20000
```

Related Commands

Command	Description
server trigger	Configure static server triggers for specific RAS messages to be forwarded to a specified server.

Command	Description
show gatekeeper servers	Displays the triggers configured on the gatekeeper.

server routing

To specify the type of circuit messages sent to the Gatekeeper Transaction Message Protocol (GKTMP) server, use the **server routing**command in gatekeeper configuration mode. To return to the default, use the **no** form of this command.

server routing {**both** | **carrier** | **trunk-group**}
no server routing {**both** | **carrier** | **trunk-group**}

Syntax Description

both	Sends both types of information in GKTMP messages.
carrier	Sends only carrier information in GKTMP messages. This is the default.
trunk -group	Sends only trunk-group information in GKTMP messages.

Command Default

Carrier

Command Modes

Gatekeeper configuration (config-gk)

Command History

Release	Modification
12.2(11)T	This command was introduced.

Usage Guidelines

Use this command to route carrier and trunk-group messages from the gatekeeper to the GKTMP server.

The **carrier**keyword sends the "I" and "J" tags in the GKTMP messages. The **trunk-group**keyword sends the "P" and "Q" tags in the GKTMP messages. The **both**keyword sends both sets of tags.

Examples

The following example enables trunk-group information to be sent in GKTMP messages from the gatekeeper:

```
Router(config)# gatekeeper
Router(config-gk)# server routing trunk-group
```

Related Commands

Command	Description
show gatekeeper servers	Displays the triggers configured on the gatekeeper.

server trigger arq

To configure the admission request (ARQ) trigger statically on the gatekeeper, use the **server trigger arq**command in gatekeeper configuration mode. Submode commands are available after the **server trigger arq**command is entered. To delete a single static trigger on the gatekeeper, use the **no** form of this command. To delete all static triggers on the gatekeeper, use the **all**form of this command.

server trigger arq *gkid priority server-id server-ip-address server-port*
no server trigger arq *gkid priority server-id server-ip-address server-port*
no server trigger all

Syntax Description

all	Deletes all CLI-configured triggers.
gkid	Local gatekeeper identifier.
priority	Priority for each trigger. Range is from 1 to 20; 1 is the highest priority.
server -id	ID number of the external application.
server -ip-address	IP address of the server.
server -port	Port on which the Cisco IOS gatekeeper listens for messages from the external server connection.

After the command is entered, the software enters a submode that permits you to configure additional filters on the reliability, availability, and serviceability (RAS) message. These filters are optional, and you may configure any of them, one per command line.

info -only	Use to indicate to the Cisco IOS gatekeeper that messages that meet the specified trigger parameters should be sent to the GKTMP server application as notifications only and that the gatekeeper should not wait for a response from the Gatekeeper Transaction Message Protocol (GKTMP) server application.
shutdown	Use to temporarily disables a trigger. The gatekeeper does not consult triggers in a shutdown state when determining what message to forward to the GKTMP server application.

destination -info e164 | **email-id** | **h323-id** *value*	Use to send ARQ RAS messages containing a specified destination to the GKTMP server application. Configure one of the following conditions
	• **e164** -- Destination is an E.164 address.
	• **email -id**-- Destination is an e-mail ID.
	• **h323 -id**-- Destination is an H.323 ID.
	• *value* -- Value against which to compare the destination address in the RAS messages. For E.164 addresses, the following wildcards can be used:
	  • A trailing series of periods, each of which represents a single character.
	  • A trailing asterisk, which represents one or more characters.

redirect -reason *reason-number*	Use to send ARQ RAS messages containing a specific redirect reason to the GKTMP server application. • *reason -number*-- Range is from 0 to 65535. Currently-used values are: • 0 -- Unknown reason. • 1 -- Call forwarding busy or called DTE busy. • 2 -- Call forwarded; no reply. • 4 -- Call deflection. • 9 -- Called DTE out of order. • 10 -- Call forwarding by the called DTE. • 15 -- Call forwarding unconditionally.

Command Default

No trigger servers are set.

Command Modes

Gatekeeper configuration(config-gk)

Command History

Release	Modification
12.1(1)T	This command was introduced.
12.2(11)T	This command was implemented on the Cisco 2600 series, Cisco 3600 series, Cisco 3700 series, Cisco 7200 series, and Cisco MC3810. The **irr**trigger was added.

Usage Guidelines

Use this command and its optional submode commands to configure the admission request (ARQ) static server trigger. The gatekeeper checks incoming gateway ARQ messages for the configured trigger information. If an incoming ARQ message contains the specified trigger information, the gatekeeper sends the ARQ message to the GKTMP server application. In addition, the gatekeeper processes the message according to its programmed instructions. If the ARQ message does not contain the specified information, the gatekeeper processes the message but does not send it to the GKTMP server application.

If no submode commands are configured for the ARQ messages, the gatekeeper sends all ARQ messages to the GKTMP server application.

If the gatekeeper receives an ARQ trigger registration message that contains several trigger conditions, the conditions are treated as "OR" conditions. In other words, if an incoming ARQ RAS message meets any one of the conditions, the gatekeeper sends the RAS message to the GKTMP server.

If the gatekeeper receives two ARQ trigger registration messages with the same priority for the same GKTMP server, the gatekeeper retains the second registration and discards the first one. If the gatekeeper receives two ARQ trigger registration messages with different priorities for the same GKTMP server, the gatekeeper checks incoming ARQ messages against the conditions on the higher priority registration before using the lower priority registration. If the gatekeeper receives more than one ARQ trigger registration message with the same priority but for different GKTMP servers, the gatekeeper retains all of the registrations.

The **no** form of the command removes the trigger definition from the Cisco IOS gatekeeper with all statically configured conditions under that trigger.

Examples

The following example configures a trigger registration on gatekeeper "sj.xyz.com" to send all ARQ messages to GKTMP server "Server-123":

```
Router(config-gk)# server trigger arq sj.xyz.com 1 Server-123 1.14.93.130 1751
Router(config-gk_arqtrigger)# exit
```

The following example configures an ARQ trigger registration on gatekeeper "alpha", which sends to GKTMP server "Server-west" any ARQ message that contains H.323 ID "3660-gw1", e-mail ID "joe.xyz.com", or a redirect reason 1. All other ARQ messages are not sent to the GKTMP server application.

```
Router(config-gk)# server trigger arq alpha 1 Server-west 10.10.10.10 1751
Router(config-gk-arqtrigger)# destination-info h323-id 3660-gw1
Router(config-gk-arqtrigger)# destination-info email-id joe.xyz.com
Router(config-gk-arqtrigger)# redirect-reason 1
Router(config-gk-arqtrigger# exit
```

If the ARQ registration message defined above for gatekeeper "alpha" is configured and the gatekeeper receives the following trigger registration:

```
Router(config-gk)# server trigger arq alpha 2 Server-west 10.10.10.10 1751
Router(config-gk_arqtrigger)# destination-info e164 1800....
Router(config-gk_arqtrigger)# exit
```

Then gatekeeper "alpha" checks all incoming ARQ messages for the destination H.323 ID, e-mail ID, or redirect reason before checking for the E.164 address 1800 (for example, 18005551212). If any one of those conditions is met, the gatekeeper sends the ARQ message to the GKTMP server "Server-west".

If the second gatekeeper "alpha" ARQ trigger registration had been defined with a priority 1 instead of priority 2, the second server trigger definition would have overridden the first one. In other words, the gatekeeper "alpha" would send to GKTMP server "Server-west" only those ARQ messages that contain a destination E.164 address that starts with 1800. All other ARQ messages would not be sent to the GKTMP server.

Related Commands

Command	Description
server registration-port	Configures the server listening port on the gatekeeper.
show gatekeeper servers	Displays the triggers configured on the gatekeeper.

server trigger brq

To configure the bandwidth request (BRQ) trigger statically on the gatekeeper, use the **server trigger brq**command in gatekeeper configuration mode. Submode commands are available after entering the **server trigger brq**command. To delete a single static trigger on the gatekeeper, use the **no** form of this command. To delete all static triggers on the gatekeeper, use the **all**form of the command.

server trigger brq *gkid priority server-id server-ip-address server-port*
no server trigger brq *gkid priority server-id server-ip-address server-port*
no server trigger all

Syntax Description

all	Deletes all CLI-configured triggers.
gkid	Local gatekeeper identifier.
priority	Priority for each trigger. Range is from 1 to 20; 1 is the highest priority.
server -id	ID number of the external application.
server -ip-address	IP address of the server.
server -port	Port on which the Cisco IOS gatekeeper listens for messages from the external server connection.

After the command is entered, the software enters a submode that permits you to configure additional filters on the reliability, availability, and serviceability (RAS) message. These filters are optional, and you may configure any of them, one per command line.

info -only	Use to indicate to the gatekeeper that messages that meet the specified trigger parameters should be sent to the Gatekeeper Transaction Message Protocol (GKTMP) server application as notifications only and that the gatekeeper should not wait for a response from the GKTMP server application.
redirect -reason *reason-number*	Use to send BRQ RAS messages containing a specific redirect reason to the GKTMP server application. • *reason-number*-- Range is from 0 to 65535. Currently used values are as follows: • 0 -- Unknown reason. • 1 -- Call forwarding busy or called DTE busy. • 2 -- Call forwarded; no reply. • 4 -- Call deflection. • 9 -- Called DTE out of order. • 10 -- Call forwarding by the called DTE. • 15 -- Call forwarding unconditionally.
shutdown	Use to temporarily disable a trigger. The gatekeeper does not consult triggers in a shutdown state when determining what message to forward to the GKTMP server application.

Command Default

No trigger servers are set.

Command Modes

Gatekeeper configuration (config-gk)

Command History

Release	Modification
12.2(2)XB	This command was introduced.
12.2(11)T	This the command was implemented on the following platforms: Cisco 2600 series, Cisco 3600 series, Cisco 3700 series, Cisco 7200 series, and Cisco MC3810. The **irr**trigger was added.

Usage Guidelines

Use this command and its optional submode commands to configure the bandwidth request (BRQ) static server trigger. The gatekeeper checks incoming gateway BRQ messages for the configured trigger information. If an incoming BRQ message contains the specified trigger information, the gatekeeper sends the BRQ message to the GKTMP server application. In addition, the gatekeeper processes the message according to its programmed instructions. If the BRQ message does not contain the specified information, the gatekeeper processes the message but does not send it to the GKTMP server application.

If no submode commands are configured for the BRQ messages, the gatekeeper sends all BRQ messages to the GKTMP server application.

If the gatekeeper receives BRQ trigger registration message that contains several trigger conditions, the conditions are treated as "OR" conditions. In other words, if an incoming BRQ RAS message meets any one of the conditions, the gatekeeper sends the RAS message to the GKTMP server.

If the gatekeeper receives two BRQ trigger registration messages with the same priority for the same GKTMP server, the gatekeeper retains the second registration and discards the first one. If the gatekeeper receives two BRQ trigger registration messages with different priorities for the same GKTMP server, the gatekeeper checks incoming BRQ messages against the conditions on the higher priority registration before using the lower priority registration. If the gatekeeper receives more than one BRQ trigger registration message with the same priority but for different GKTMP servers, the gatekeepers retains all of the registrations.

The **no** form of the command removes the trigger definition from the Cisco IOS gatekeeper with all statically configured conditions under that trigger.

Examples

The following example configures a trigger registration on gatekeeper "sj.xyz.com" to send all BRQ messages to GKTMP server "Server-123":

```
Router(config-gk)# server trigger brq sj.xyz.com 1 Server-123 1.14.93.130 1751
Router(config-gk_brqtrigger)# exit
```

The following example configures BRQ trigger registration on gatekeeper "alpha", which sends to GKTMP server "Server-west" any BRQ message containing redirect reason 1 or redirect reason 2. All other BRQ messages are not sent to the GKTMP server application.

```
Router(config-gk)# server trigger brq alpha 1 Server-west 10.10.10.10 1751
Router(config-gk-brqtrigger)# redirect-reason 1
Router(config-gk-brqtrigger)# redirect-reason 2
Router(config-gk-brqtrigger# exit
```

If the BRQ registration message defined above for gatekeeper "alpha" is configured and the gatekeeper receives the following trigger registration:

```
Router(config-gk)# server trigger brq alpha 2 Server-west 10.10.10.10 1751
Router(config-gk_brqtrigger)# redirect-reason 10
Router(config-gk_brqtrigger)# exit
```

Then gatekeeper "alpha" checks all incoming BRQ messages for redirect reasons 1 or 2 before checking for redirect reason 10. If any one of those conditions is met, the gatekeeper sends the BRQ message to the GKTMP server "Server-west".

If the second gatekeeper "alpha" BRQ trigger registration had been defined with a priority 1 instead of priority 2, then the second server trigger definition would have overridden the first one. In other words, the gatekeeper "alpha" would send to GKTMP server "Server-west" only those BRQ messages that contain a redirect reason 10. All other BRQ messages would not be sent to the GKTMP server.

Related Commands

Command	Description
server registration-port	Configures the server listening port on the gatekeeper.
show gatekeeper servers	Displays the triggers configured on the gatekeeper.

server trigger drq

To configure the disengage request (DRQ) trigger statically on the gatekeeper, use the **server trigger drq**command in gatekeeper configuration mode. Submode commands are available after entering the **server trigger drq**command. To delete a single static trigger on the gatekeeper, use the **no** form of this command. To delete all static triggers on the gatekeeper, use the **all**form of the command.

server trigger drq *gkid priority server-id server-ip-address server-port*
no server trigger drq *gkid priority server-id server-ip-address server-port*
no server trigger all

Syntax Description

all	Deletes all CLI-configured triggers.
gkid	Local gatekeeper identifier.
priority	Priority for each trigger. Range is from 1 to 20; 1 is the highest priority.
server -id	ID number of the external application.
server -ip-address	IP address of the server.
server -port	Port on which the Cisco IOS gatekeeper listens for messages from the external server connection.

After the command is entered, the software enters a submode that permits you to configure additional filters on the Reliability, Availability, and Serviceability (RAS) message. These filters are optional, and you may configure any of them, one per command line.

info -only	Use to indicate to the gatekeeper that messages that meet the specified trigger parameters should be sent to the Gatekeeper Transaction Message Protocol (GKTMP) server application as notifications only and that the gatekeeper should not wait for a response from the GKTMP server application.

destination -info e164 | **email-id** | **h323-id** *value*	Use to send automatic repeat request (ARQ) RAS messages containing a specified destination to the GKTMP server application. Configure one of the following conditions:
	• **e164** -- Destination is an E.164 address.
	• **email -id**-- Destination is an e-mail ID.
	• **h323 -id**-- Destination is an H.323 ID.
	• *value*-- Value against which to compare the destination address in the RAS messages. For E.164 addresses, the following wildcards can be used:
	  • A trailing series of periods, each of which represents a single character.
	  • A trailing asterisk, which represents one or more characters.

call info type { **fax** | **modem** | **voice**	Use to send ARQ RAS messages containing a specified call info type to the GKTMP server application. The following types can be used: • **fax** • modem • **voice**
shutdown	Use to temporarily disable a trigger. The gatekeeper does not consult triggers in a shutdown state when determining what message to forward to the GKTMP server application.

Command Default

No trigger servers are set.

Command Modes

Gatekeeper configuration (config-gk)

Command History

Release	Modification
12.2(2)XB	This command was introduced.
12.2(11)T	This command was implemented on the following platforms: Cisco 2600 series, Cisco 3600 series, Cisco 3700 series, Cisco 7200 series, and Cisco MC3810.
12.4(4)T	The **call-info-type** submode command was added.

Usage Guidelines

Use this command and its optional submode commands to configure the disengage request (DRQ) static server trigger. The gatekeeper checks incoming gateway DRQ messages for the configured trigger information. If an incoming DRQ message contains the specified trigger information, the gatekeeper sends the DRQ message to the GKTMP server application. In addition, the gatekeeper processes the message according to its programmed instructions. If the DRQ message does not contain the specified information, the gatekeeper processes the message but does not send it to the GKTMP server application.

If no submode commands are configured for the DRQ messages, the gatekeeper sends all DRQ messages to the GKTMP server application.

If the gatekeeper receives a DRQ trigger registration message that contains several trigger conditions, the conditions are treated as "OR" conditions. In other words, if an incoming DRQ RAS message meets any one of the conditions, the gatekeeper sends the RAS message to the GKTMP server.

If the gatekeeper receives two DRQ trigger registration messages with the same priority for the same GKTMP server, the gatekeeper retains the second registration and discards the first one. If the gatekeeper receives two DRQ trigger registration messages with different priorities for the same GKTMP server, the gatekeeper checks incoming DRQ messages against the conditions on the higher priority registration before using the lower priority registration. If the gatekeeper receives more than one DRQ trigger registration message with the same priority but for different GKTMP servers, the gatekeeper retains all of the registrations.

The **no** form of the command removes the trigger definition from the Cisco IOS gatekeeper together with all statically configured conditions under that trigger.

Examples

The following example configures a trigger registration on gatekeeper "sj.xyz.com" to send all DRQ messages to GKTMP server "Server-123":

```
Router(config-gk)# server trigger drq sj.xyz.com 1 Server-123 1.14.93.130 1751
Router(config-gk_drqtrigger)# exit
```

The following example configures DRQ trigger registration on gatekeeper "alpha", which sends to GKTMP server "Server-west" any DRQ message containing an H.323 ID "3660-gw1" or e-mail ID "joe.xyz.com". All other DRQ messages are not sent to the GKTMP server application.

```
Router(config-gk)# server trigger drq alpha 1 Server-west 10.10.10.10 1751
Router(config-gk-drqtrigger)# destination-info h323-id 3660-gw1
Router(config-gk-drqtrigger)# destination-info email-id joe.xyz.com
Router(config-gk-drqtrigger# exit
```

If the DRQ registration message defined above for gatekeeper "alpha" is configured and the gatekeeper receives the following trigger registration:

```
Router(config-gk)# server trigger drq alpha 2 Server-west 10.10.10.10 1751
Router(config-gk_drqtrigger)# destination-info e164 1800....
Router(config-gk_drqtrigger)# exit
```

then gatekeeper "alpha" checks all incoming DRQ messages for the destination H.323 ID or e-mail ID before checking for the E.164 address 1800 (for example, 18005551212). If any one of those conditions is met, the gatekeeper sends the DRQ message to the GKTMP server "Server-west".

If the second gatekeeper "alpha" DRQ trigger registration had been defined with a priority 1 instead of priority 2, then the second trigger registration would have overridden the first one. In other words, the gatekeeper "alpha" would send to GKTMP server Server-west only those DRQ messages that contain a destination E.164 address starting with 1800. All other DRQ messages would not be sent to the GKTMP server.

Related Commands

Command	Description
server registration-port	Configures the server listening port on the gatekeeper.
show gatekeeper servers	Displays the triggers configured on the gatekeeper.

server trigger irr

To configure the information request response (IRR) trigger statically on the gatekeeper, use the **server trigger irr**command in gatekeeper configuration mode. Submode commands are available after entering the **server trigger irr**command. To delete a single static trigger on the gatekeeper, use the **no** form of this command. To delete all static triggers on the gatekeeper, use the **all**form of the command.

server trigger irr *gkid priority server-id server-ip-address server-port*
no server trigger irr *gkid priority server-id server-ip-address server-port*
no server trigger all

Syntax Description

all	Deletes all CLI-configured triggers.
gkid	Local gatekeeper identifier.
priority	Priority for each trigger. Range is from 1 to 20; 1 is the highest priority.
server -id	ID number of the external application.
server -ip-address	IP address of the server.
server -port	Port on which the Cisco IOS gatekeeper listens for messages from the external server connection.

After the command is entered, the software enters a submode that permits you to configure additional filters on the reliability, availability, and serviceability (RAS) message. These filters are optional, and you may configure any of them, one per command line.

destination -info e164 | **email-id** | **h323-id** *value*	Use to send IRR RAS messages containing a specified destination to the GKTMP server application. Configure one of the following conditions:
	• **e164** -- Destination is an E.164 address.
	• **email -id**-- Destination is an e-mail ID.
	• **h323 -id**-- Destination is an H.323 ID.
	• *value*-- Value against which to compare the destination address in the RAS messages. For E.164 addresses, the following wildcards can be used:
	  • A trailing series of periods, each of which represents a single character.
	  • A trailing asterisk, which represents one or more characters.

info -only	Use to indicate to the gatekeeper that messages that meet the specified trigger parameters should be sent to the Gatekeeper Transaction Message Protocol (GKTMP) server application as notifications only and that the gatekeeper should not wait for a response from the GKTMP server application.

redirect -reason *reason-number*	Use to send IRR RAS messages containing a specific redirect reason to the GKTMP server application. • *reason -number*--Range is from 0 to 65535. Currently used values are the following: • 0 -- Unknown reason. • 1 -- Call forwarding busy or called DTE busy. • 2 -- Call forwarded; no reply. • 4 -- Call deflection. • 9 -- Called DTE out of order. • 10 -- Call forwarding by the called DTE. • 15 -- Call forwarding unconditionally.
shutdown	Use to temporarily disable a trigger. The gatekeeper does not consult triggers in a shutdown state when determining what message to forward to the GKTMP server application.

Command Default

No trigger servers are set.

Command Modes

Gatekeeper configuration (config-gk)

Command History

Release	Modification
12.1(1)T	This command was introduced.
12.2(11)T	This command was implemented on the following platforms: Cisco 2600 series, Cisco 3600 series, Cisco 3700 series, Cisco 7200 series, and Cisco MC3810. The **irr**trigger was added.

Usage Guidelines

Use this command and its optional submode commands to configure the information request response (IRR) static server trigger. The gatekeeper checks incoming gateway IRR messages for the configured trigger information. If an incoming IRR message contains the specified trigger information, the gatekeeper sends the IRR message to the GKTMP server application. In addition, the IRR message does not contain the specified information, the gatekeeper processes the message but does not send it to the GKTMP server application.

If no submode commands are configured for the IRR messages, the gatekeeper sends all IRR messages to the GKTMP server application.

If the gatekeeper receives an IRR trigger registration message that contains several trigger conditions, the conditions are treated as "OR" conditions. In other words, if an incoming IRR RAS message meets any one of the conditions, the gatekeeper sends the RAS message to the GKTMP server.

If the gatekeeper receives two IRR trigger registration messages with the same priority for the same GKTMP server, the gatekeeper retains the second registration and discards the first one. If the gatekeeper receives two IRR trigger registration messages with different priorities for the same GKTMP server, the gatekeeper checks incoming IRR messages against the conditions on the higher priority registration before using the lower priority registration. If the gatekeeper receives more than one IRR trigger registration message with the same priority but for different GKTMP servers, the gatekeepers retains all of the registrations.

The **no** form of the command removes the trigger definition from the Cisco IOS gatekeeper with all statically configured conditions under that trigger.

Examples

The following example configures a trigger registration on gatekeeper "sj.xyz.com" to send all IRR messages to GKTMP server "Server-123":

```
Router(config-gk)# server trigger irr sj.xyz.com 1 Server-123 1.14.93.130 1751
Router(config-gk_irrtrigger)# exit
```

The following example configures an IRR trigger registration on gatekeeper "alpha", which send to GKTMP server "Server-west" any IRR message containing an H.323 ID "3660-gw1", e-mail ID "joe.xyz.com, or a redirect reason 1. All other IRR messages are not sent to the GKTMP server application.

```
Router(config-gk)# server trigger irr alpha 1 Server-west 10.10.10.10 1751
Router(config-gk-irrtrigger)# destination-info h323-id 3660-gw1
Router(config-gk-irrtrigger)# destination-info email-id joe.xyz.com
Router(config-gk-irrtrigger)# redirect-reason 1
Router(config-gk-irrtrigger# exit
```

If the IRR registration message defined above for gatekeeper "alpha" is configured and the gatekeeper receives the following trigger registration:

```
Router(config-gk)# server trigger irr alpha 2 Server-west 10.10.10.10 1751
Router(config-gk_irrtrigger)# destination-info e164 1800....
Router(config-gk_irrtrigger)# exit
```

Then gatekeeper "alpha" checks all incoming IRR messages for the destination H.323 ID, e-mail ID, or redirect reason before checking for the E.164 address 1800 (for example, 18005551212). If any one of those conditions is met, the gatekeeper sends the IRR message to the GKTMP server "Server-west".

If the second gatekeeper "alpha" IRR trigger registration had been defined with a priority 1 instead of priority 2, then the second server trigger definition would have overridden the first one. In other words, the gatekeeper "alpha" would send to GKTMP server "Server-west" only those IRR messages that contain a destination E.164 address starting with 1800. All other IRR messages would not be sent to the GKTMP server.

Related Commands

Command	Description
server registration-port	Configures the server listening port on the gatekeeper.
show gatekeeper servers	Displays the triggers configured on the gatekeeper.

server trigger lcf

To configure the location confirm (LCF) trigger statically on the gatekeeper, use the **server trigger lcf**command in gatekeeper configuration mode. Submode commands are available after entering the **server trigger lcf**command. To delete a single static trigger on the gatekeeper, use the **no** form of this command. To delete all static triggers on the gatekeeper, use the **all**form of the command.

server trigger lcf *gkid priority server-id server-ip-address server-port*
no server trigger lcf *gkid priority server-id server-ip-address server-port*
no server trigger all

Syntax Description

all	Deletes all CLI-configured triggers.
gkid	Local gatekeeper identifier.
priority	Priority for each trigger. Range is from 1 to 20; 1 is the highest priority.
server -id	ID number of the external application.
server -ip-address	IP address of the server.
server -port	Port on which the Cisco IOS gatekeeper listens for messages from the external server connection.

After the command is entered, the software enters a submode that permits you to configure additional filters on the RAS message. These filters are optional, and you may configure any of them, one per command line.

destination -info e164 | **email-id** | **h323-id** *value*	Use to send LCF RAS messages containing a specified destination to the GKTMP server application. Configure one of the following conditions:
	• **e164** -- Destination is an E.164 address.
	• **email -id**-- Destination is an e-mail ID.
	• **h323 -id**-- Destination is an H.323 ID.
	• *value*-- Value against which to compare the destination address in the RAS messages. For E.164 addresses, the following wildcards can be used:
	  • A trailing series of periods, each of which represents a single character.
	  • A trailing asterisk, which represents one or more characters.

info -only	Use to indicate to the gatekeeper that messages that meet the specified trigger parameters should be sent to the Gatekeeper Transaction Message Protocol (GKTMP) server application as notifications only and that the gatekeeper should not wait for a response from the GKTMP server application.

remote -ext-address e164 *value*	Use to send LCF RAS messages that contain a specified remote extension address to the GKTMP server application.
	• **e164** --Remote extension address is an E.164 address.
	• *value* --Value against which to compare the destination address in the RAS messages. The following wildcards can be used:
	  • A trailing series of periods, each of which represents a single character.
	  • A trailing asterisk, which represents one or more characters.

shutdown	Use to temporarily disable a trigger. The gatekeeper does not consult triggers in a shutdown state when determining what message to forward to the GKTMP server application.

Command Default

No trigger servers are set.

Command Modes

Gatekeeper configuration (config-gk)

Command History

Release	Modification
12.1(1)T	This command was introduced.
12.2(11)T	This command was implemented on the following platforms: Cisco 2600 series, Cisco 3600 series, Cisco 3700 series, Cisco 7200 series, and Cisco MC3810. The **irr**trigger was added.

Usage Guidelines

Use this command and its optional submode commands to configure the location confirm (LCF) static server trigger. The gatekeeper checks incoming gateway LCF messages for the configured trigger information. If an incoming LCF message contains the specified trigger information, the gatekeeper sends the LCF message to the GKTMP server application. In addition, the gatekeeper processes the message according to its programmed instructions. If the LCF message does not contain the specified information, the gatekeeper processes the message but does not send it to the GKTMP server application.

If no submode commands are configured for the LCF messages, the gatekeeper sends all LCF messages to the GKTMP server application.

If the gatekeeper receives an LCF trigger registration message that contains several trigger conditions, the conditions are treated as "OR" conditions. In other words, if an incoming LCF RAS message meets any one of the conditions, the gatekeeper sends the RAS message to the GKTMP server.

If the gatekeeper receives two LCF trigger registration messages with the same priority for the same GKTMP server, the gatekeeper retains the second registration and discards the first one. If the gatekeeper receives two LCF trigger registration messages with different priorities for the same GKTMP server, the gatekeeper checks incoming LCF messages against the conditions on the higher priority registration before using the lower priority registration. If the gatekeeper receives more than one LCF trigger registration message with the same priority but for different GKTMP servers, the gatekeepers retains all of the registrations.

The **no** form of the command removes the trigger definition from the Cisco IOS gatekeeper with all statically configured conditions under that trigger.

Examples

The following example configures a trigger registration on gatekeeper "sj.xyz.com" to send all LCF messages to GKTMP server "Server-123":

```
Router(config-gk)# server trigger lcf sj.xyz.com 1 Server-123 1.14.93.130 1751
Router(config-gk_lcftrigger)# exit
```

The following example configures an LCF trigger registration on gatekeeper "alpha", which send to GKTMP server "Server-west" any LCF message containing an H.323 ID "3660-gw1", e-mail ID joe.xyz.com, or a remote extension address starting with 1408. All other LCF messages are not sent to the GKTMP server application.

```
Router(config-gk)# server trigger lcf alpha 1 Server-west 10.10.10.10 1751
Router(config-gk-lcftrigger)# destination-info h323-id 3660-gw1
Router(config-gk-lcftrigger)# destination-info email-id joe.xyz.com
Router(config-gk-lcftrigger)# remote-ext-address e164 1408....
Router(config-gk-lcftrigger# exit
```

If the LCF registration message defined above for gatekeeper "alpha" is configured and the gatekeeper receives the following trigger registration:

```
Router(config-gk)# server trigger lcf alpha 2 Server-west 10.10.10.10 1751
Router(config-gk_lcftrigger)# remote-ext-address e164 1800....
Router(config-gk_lcftrigger)# exit
```

then gatekeeper "alpha" checks all incoming LCF messages for the destination H.323 ID, e-mail ID, or remote extension address 1408 before checking for the remote extension address 1800 (for example, 18005551212). If any one of those conditions is met, the gatekeeper sends the LCF message to the GKTMP server "Server-west".

If the second gatekeeper "alpha" LCF trigger registration had been defined with a priority 1 instead of priority 2, then the second trigger registration would have overridden the first one. In other words, the gatekeeper "alpha" would send to GKTMP server "Server-west" only those LCF messages that contain a remote extension address E.164 address starting with 1800. All other LCF messages would not be sent to the GKTMP server.

Related Commands

Command	Description
server registration-port	Configures the server listening port on the gatekeeper.
show gatekeeper servers	Displays the triggers configured on the gatekeeper.

server trigger lrj

To configure the location reject (LRJ) trigger statically on the gatekeeper, use the **server trigger lrj**command in gatekeeper configuration mode. Submode commands are available after entering the **server trigger lrj**command. To delete a single static trigger on the gatekeeper, use the **no** form of this command. To delete all static triggers on the gatekeeper, use the **all**form of the command.

server trigger lrj *gkid priority server-id server-ip-address server-port*
no server trigger lrj *gkid priority server-id server-ip-address server-port*
no server trigger all

Syntax Description

all	Deletes all CLI-configured triggers.
gkid	Local gatekeeper identifier.
priority	Priority for each trigger. Range is from 1 to 20; 1 is the highest priority.
server -id	ID number of the external application.
server -ip-address	IP address of the server.
server -port	Port on which the gatekeeper listens for messages from the external server connection.

After the command is entered, the software enters a submode that permits you to configure additional filters on the reliability, availability, and serviceability (RAS) message. These filters are optional, and you may configure any of them, one per command line.

destination -info e164 | **email-id** | **h323-id** *value*	Use to send LRJ RAS messages containing a specified destination to the GKTMP server application. Configure one of the following conditions:
	• **e164** -- Destination is an E.164 address.
	• **email -id**-- Destination is an e-mail ID.
	• **h323 -id**-- Destination is an H.323 ID.
	• *value*-- Value against which to compare the destination address in the RAS messages. For E.164 addresses, the following wildcards can be used:
	  • A trailing series of periods, each of which represents a single character.
	  • A trailing asterisk, which represents one or more characters.

info -only	Use to indicate to the gatekeeper that messages that meet the specified trigger parameters should be sent to the Gatekeeper Transaction Message Protocol (GKTMP) server application as notifications only and that the gatekeeper should not wait for a response from the GKTMP server application.
shutdown	Use to temporarily disable a trigger. The gatekeeper does not consult triggers in a shutdown state when determining what message to forward to the GKTMP server application.

Command Default

No trigger servers are set.

Command Modes

Gatekeeper configuration (config-gk)

Command History

Release	Modification
12.1(1)T	This command was introduced.
12.2(11)T	This command was implemented on the following platforms: Cisco 2600 series, Cisco 3600 series, Cisco 3700 series, Cisco 7200 series, and Cisco MC3810.

Usage Guidelines

Use this command and its optional submode commands to configure the location reject (LRJ) static server trigger. The gatekeeper checks incoming gateway LRJ messages for the configured trigger information. If an incoming LRJ message contains the specified trigger information, the gatekeeper sends the LRJ message to the GKTMP server application. In addition, the gatekeeper processes the message according to its programmed instructions. If the LRJ message does not contain the specified information, the gatekeeper processes the message but does not send it to the GKTMP server application.

If no submode commands are configured for the LRJ messages, the gatekeeper sends all LRJ messages to the GKTMP server application.

If the gatekeeper receives an LRJ trigger registration message that contains several trigger conditions, the conditions are treated as "OR" conditions. In other words, if an incoming LRJ RAS message meets any one of the conditions, the gatekeeper sends the RAS message to the GKTMP server.

If the gatekeeper receives two LRJ trigger registration messages with the same priority for the same GKTMP server, the gatekeeper retains the second registration and discards the first one. If the gatekeeper receives two LRJ trigger registration messages with different priorities for the same GKTMP server, the gatekeeper checks incoming LRJ messages against the conditions on the higher priority registration before using the lower priority registration. If the gatekeeper receives more than one LRJ trigger registration message with the same priority but for different GKTMP servers, the gatekeepers retains all of the registrations.

The **no** form of the command removes the trigger definition from the Cisco IOS gatekeeper with all statically configured conditions under that trigger.

Examples

The following example configures a trigger registration on gatekeeper "sj.xyz.com" to send all LRJ messages to GKTMP server "Server-123":

```
Router(config-gk)# server trigger lrj sj.xyz.com 1 Server-123 1.14.93.130 1751
Router(config-gk_lrjtrigger)# exit
```

The following example configures an LRJ trigger registration on gatekeeper "alpha", which send to GKTMP server "Server-west" any LRJ message containing an H.323 ID "3660-gw1" or e-mail ID joe.xyz.com. All other LRJ messages are not sent to the GKTMP server application.

```
Router(config-gk)# server trigger lrj alpha 1 Server-west 10.10.10.10 1751
Router(config-gk-lrjtrigger)# destination-info h323-id 3660-gw1
Router(config-gk-lrjtrigger)# destination-info email-id joe.xyz.com
Router(config-gk-lrjtrigger# exit
```

If the LRJ registration message defined above for gatekeeper "alpha" is configured and the gatekeeper receives the following trigger registration:

```
Router(config-gk)# server trigger lrj alpha 2 Server-west 10.10.10.10 1751
```

```
Router(config-gk_lrjtrigger)# destination-info e164 1800....
Router(config-gk_lrjtrigger)# exit
```

then gatekeeper "alpha" checks all incoming LRJ messages for the destination H.323 ID or email ID before checking for the E.164 address 1800 (for example, 18005551212). If any one of those conditions is met, the gatekeeper sends the LRJ message to the GKTMP server "Server-west".

If the second gatekeeper "alpha" LRJ trigger registration had been defined with a priority 1 instead of priority 2, then the second trigger registration would have overridden the first one. In other words, the gatekeeper "alpha" would send to GKTMP server "Server-west" only those LRJ messages that contain a destination E.164 address starting with 1800. All other LRJ messages would not be sent to the GKTMP server.

Related Commands

Command	Description
server registration-port	Configures the server listening port on the gatekeeper.
show gatekeeper servers	Displays the triggers configured on the gatekeeper.

server trigger lrq

To configure the location request (LRQ) trigger statically on the gatekeeper, use the **server trigger lrq**command in gatekeeper configuration mode. Submode commands are available after entering the **server trigger lrq**command. To delete a single static trigger on the gatekeeper, use the **no** form of this command. To delete all static triggers on the gatekeeper, use the **all**form of the command.

server trigger lrq *gkid priority server-id server-ip-address server-port*
no server trigger lrq *gkid priority server-id server-ip-address server-port*
no server trigger all

Syntax Description

all	Deletes all CLI-configured triggers.
gkid	Local gatekeeper identifier.
priority	Priority for each trigger. Range is from 1 to 20; 1 is the highest priority.
server -id	ID number of the external application.
server -ip-address	IP address of the server.
server -port	Port on which the Cisco IOS gatekeeper listens for messages from the external server connection.

After the command is entered, the software enters a submode that permits you to configure additional filters on the reliability, availability, and serviceability (RAS) message. These filters are optional, and you may configure any of them, one per command line.

destination -info e164 | **email-id** | **h323-id** *value*	Use to send LRQ RAS messages containing a specified destination to the GKTMP server application. Configure one of the following conditions:
	• **e164** -- Destination is an E.164 address.
	• **email -id**-- Destination is an e-mail ID.
	• **h323 -id**-- Destination is an H.323 ID.
	• *value*-- Value against which to compare the destination address in the RAS messages. For E.164 addresses, the following wildcards can be used:
	  • A trailing series of periods, each of which represents a single character.
	  • A trailing asterisk, which represents one or more characters.

info -only	Use to indicate to the gatekeeper that messages that meet the specified trigger parameters should be sent to the Gatekeeper Transaction Message Protocol (GKTMP) server application as notifications only and that the gatekeeper should not wait for a response from the GKTMP server application.

redirect -reason *reason-number*	Use to send LRQ RAS messages containing a specific redirect reason to the GKTMP server application. • *reason -number*--Range is from 0 to 65535. Currently used values are the following: • 0 -- Unknown reason. • 1 -- Call forwarding busy or called DTE busy. • 2 -- Call forwarded; no reply. • 4 -- Call deflection. • 9 -- Called DTE out of order. • 10 -- Call forwarding by the called DTE. • 15 -- Call forwarding unconditionally.
shutdown	Use to temporarily disable a trigger. The gatekeeper does not consult triggers in a shutdown state when determining what message to forward to the GKTMP server application.

Command Default

No trigger servers are set.

Command Modes

Gatekeeper configuration (config-gk)

Command History

Release	Modification
12.1(1)T	This command was introduced.
12.2(11)T	This command was implemented on the following platforms: Cisco 2600 series, Cisco 3600 series, Cisco 3700 series, Cisco 7200 series, and Cisco MC3810.

Usage Guidelines

Use this command and its optional submode commands to configure the location request (LRQ) static server trigger. The gatekeeper checks incoming gateway LRQ messages for the configured trigger information. If an incoming LRQ message contains the specified trigger information, the gatekeeper sends the LRQ message to the GKTMP server application. In addition, the gatekeeper processes the message according to its programmed instructions. If the LRQ message does not contain the specified information, the gatekeeper processes the message but does not send it to the GKTMP server application.

If no submode commands are configured for the LRQ messages, the gatekeeper sends all LRQ messages to the GKTMP server application.

If the gatekeeper receives an LRQ trigger registration message that contains several trigger conditions, the conditions are treated as "OR" conditions. In other words, if an incoming LRQ RAS message meets any one of the conditions, the gatekeeper sends the RAS message to the GKTMP server.

If the gatekeeper receives two LRQ trigger registration messages with the same priority for the same GKTMP server, the gatekeeper retains the second registration and discards the first one. If the gatekeeper receives two LRQ trigger registration messages with different priorities for the same GKTMP server, the gatekeeper checks incoming LRQ messages against the conditions on the higher priority registration before using the lower priority registration. If the gatekeeper receives more than one LRQ trigger registration message with the same priority but for different GKTMP servers, the gatekeepers retains all of the registrations.

The **no** form of the command removes the trigger definition from the Cisco IOS gatekeeper with all statically configured conditions under that trigger.

Examples

The following example configures a trigger registration on gatekeeper "sj.xyz.com" to send all LRQ messages to GKTMP server "Server-123":

```
Router(config-gk)# server trigger lrq sj.xyz.com 1 Server-123 1.14.93.130 1751
Router(config-gk_lrqtrigger)# exit
```

The following example configures an LRQ trigger registration on gatekeeper "alpha", which sends to GKTMP server "Server-west" any LRQ message containing an H.323 ID "3660-gw1", e-mail ID joe.xyz.com, or a redirect reason 1. Other LRQ messages are not sent to the GKTMP server application.

```
Router(config-gk)# server trigger lrq alpha 1 Server-west 10.10.10.10 1751
Router(config-gk-lrqtrigger)# destination-info h323-id 3660-gw1
Router(config-gk-lrqtrigger)# destination-info email-id joe.xyz.com
Router(config-gk-lrqtrigger)# redirect-reason 1
Router(config-gk-lrqtrigger# exit
```

If the LRQ registration message defined above for gatekeeper "alpha" is configured and the gatekeeper receives the following trigger registration:

```
Router(config-gk)# server trigger lrq alpha 2 Server-west 10.10.10.10 1751
Router(config-gk_lrqtrigger)# destination-info e164 1800....
Router(config-gk_lrqtrigger)# exit
```

then gatekeeper "alpha" checks all incoming LRQ messages for the destination H.323 ID, email ID, or redirect reason before checking for the E.164 address 1800 (for example, 18005551212). If any one of those conditions is met, the gatekeeper sends the LRQ message to the GKTMP server "Server-west".

If the second gatekeeper "alpha" LRQ trigger registration had been defined with a priority 1 instead of priority 2, then the second server trigger definition would have overridden the first one. In other words, the gatekeeper "alpha" would send to GKTMP server "Server-west" only those LRQ messages that contain a destination E.164 address starting with 1800. All other LRQ messages would not be sent to the GKTMP server.

Related Commands

Command	Description
server registration-port	Configures the server listening port on the gatekeeper.
show gatekeeper servers	Displays the triggers configured on the gatekeeper.

server trigger rai

To configure the resources available indicator (RAI) trigger statically on the gatekeeper, use the **server trigger rai**command in gatekeeper configuration mode. Submode commands are available after entering the **server trigger rai**command. To delete a single static trigger on the gatekeeper, use the **no** form of this command. To delete all static triggers on the gatekeeper, use the **all**form of the command.

server trigger rai *gkid priority server-id server-ip-address server-port*
no server trigger rai *gkid priority server-id server-ip-address server-port*
no server trigger all

Syntax Description

all	Deletes all CLI-configured triggers.
gkid	Local gatekeeper identifier.
priority	Priority for each trigger. Range is from 1 to 20; 1 is the highest priority.
server -id	ID number of the external application.
server -ip-address	IP address of the server.
server -port	Port on which the Cisco IOS gatekeeper listens for messages from the external server connection.

After the command is entered, the software enters a submode that permits you to configure additional filters on the reliability, availability, and serviceability (RAS) message. These filters are optional, and you may configure any of them, one per command line.

endpoint -type *value*	Use to send RAI RAS messages that contain a particular endpoint type to the GKTMP server application. • *value* --Value against which to compare the endpoint type in the RAS messages. Valid endpoint types are the following: • **gatekeeper**--Endpoint is an H.323 gatekeeper. • **h320-gateway**--Endpoint is an H.320 gateway. • **mcu**--Endpoint is a multipoint control unit (MCU). • **other-gateway**--Endpoint is another type of gateway not specified on this list. • **proxy**--Endpoint is an H.323 proxy. • **terminal**--Endpoint is an H.323 terminal. • **voice-gateway**--Endpoint is a voice gateway.
info -only	Use to indicate to the gatekeeper that messages that meet the specified trigger parameters should be sent to the Gatekeeper Transaction Message Protocol (GKTMP) server application as notifications only and that the gatekeeper should not wait for a response from the GKTMP server application.
shutdown	Use to temporarily disable a trigger. The gatekeeper does not consult triggers in a shutdown state when determining what message to forward to the GKTMP server application.

supported -prefix *value*	Use to send RAI RAS messages that contain a specific supported prefix to the GKTMP server application. • *value* --Value against which to compare the supported prefix in the RAS messages. The possible values are any E.164 pattern used as a gateway technology prefix. The value string can contain any of the following: 0123456789#*.

Command Default

No trigger servers are set.

Command Modes

Gatekeeper configuration (config-gk)

Command History

Release	Modification
12.1(1)T	This command was introduced.
12.2(11)T	This command was implemented on the following platforms: Cisco 2600 series, Cisco 3600 series, Cisco 3700 series, Cisco 7200 series, and Cisco MC3810. The **irr**trigger was added.

Usage Guidelines

Use this command and its optional submode commands to configure the resources available indicator (RAI) static server trigger. The gatekeeper checks incoming gateway RAI messages for the configured trigger information. If an incoming RAI message contains the specified trigger information, the gatekeeper sends the RAI message to the GKTMP server application. In addition, the gatekeeper processes the message according to its programmed instructions. If the RAI message does not contain the specified information, the gatekeeper processes the message but does not send it to the GKTMP server application.

If no submode commands are configured for the RAI messages, the gatekeeper sends all RAI messages to the GKTMP server application.

If the gatekeeper receives an RAI trigger registration message that contains several trigger conditions, the conditions are treated as "OR" conditions. In other words, if an incoming RAI RAS message meets any one of the conditions, the gatekeeper sends the RAS message to the GKTMP server.

If the gatekeeper receives two RAI trigger registration messages with the same priority for the same GKTMP server, the gatekeeper retains the second registration and discards the first one. If the gatekeeper receives two RAI trigger registration messages with different priorities for the same GKTMP server, the gatekeeper checks incoming RAI messages against the conditions on the higher priority registration before using the lower priority registration. If the gatekeeper receives more than one RAI trigger registration message with the same priority but for different GKTMP servers, the gatekeepers retains all of the registrations.

The **no** form of the command removes the trigger definition from the Cisco IOS gatekeeper with all statically configured conditions under that trigger.

Examples

The following example configures a trigger registration on gatekeeper "sj.xyz.com" to send all RAI messages to GKTMP server "Server-123":

```
Router(config-gk)# server trigger rai sj.xyz.com 1 Server-123 1.14.93.130 1751
Router(config-gk_raitrigger)# exit
```

The following example configures an RAI trigger registration on gatekeeper "alpha", which sends to the GKTMP server "Server-west" any RAI message that contain an MCU endpoint, an H.323 proxy endpoint, or a supported prefix 1#. All other RAI messages are not sent to the GKTMP server.

```
Router(config-gk)# server trigger rai alpha 1 Server-west 10.10.10.10 1751
Router(config-gk-raitrigger)# endpoint-type mcu
Router(config-gk-raitrigger)# endpoint-type proxy
Router(config-gk-raitrigger)# supported-prefix 1#
Router(config-gk-raitrigger# exit
```

If the RAI registration message defined above for gatekeeper "alpha" is configured and the gatekeeper receives the following trigger registration:

```
Router(config-gk)# server trigger rai alpha 2 Server-west 10.10.10.10 1751
Router(config-gk_raitrigger)# supported-prefix 1234*
Router(config-gk_raitrigger)# exit
```

Then gatekeeper "alpha" checks all incoming RAI messages for the MCU or H.323 proxy endpoint or the supported prefix 1# before checking for the supported prefix 1234*. If any one of those conditions is met, the gatekeeper sends the RAI message to the GKTMP server "Server-west".

If the second gatekeeper "alpha" RAI trigger registration had been defined with a priority 1 instead of priority 2, then the second trigger registration would have overridden the first one. In other words, the gatekeeper "alpha" would send to GKTMP server "Server-west" only those RAI messages that contain a supported prefix of 1234*. All other RAI messages would not be sent to the GKTMP server.

Related Commands

Command	Description
server registration-port	Configures the server listening port on the gatekeeper.
show gatekeeper servers	Displays the triggers configured on the gatekeeper.

server trigger rrq

To configure the registration request (RRQ) trigger statically on the gatekeeper, use the **server trigger rrq**command in gatekeeper configuration mode. Submode commands are available after entering the **server trigger rrq**command. To delete a single static trigger on the gatekeeper, use the **no** form of this command. To delete all static triggers on the gatekeeper, use the **all**form of the command.

server trigger rrq *gkid priority server-id server-ip-address server-port*
no server trigger rrq *gkid priority server-id server-ip-address server-port*
no server trigger all

Syntax Description

all	Deletes all CLI-configured triggers.
gkid	Local gatekeeper identifier.
priority	Priority for each trigger. Range is from 1 to 20; 1 is the highest priority.
server-id	ID number of the external application.
server -ip-address	IP address of the server.
server -port	Port on which the Cisco IOS gatekeeper listens for messages from the external server connection.

After the command is entered, the software enters a submode that permits you to configure additional filters on the reliability, availability, and serviceability (RAS) message. These filters are optional, and you may configure any of them, one per command line.

endpoint -type *value*	Use to send RRQ RAS messages containing a particular endpoint type to the GKTMP server application. • *value* --Value against which to compare the endpoint-type in the RAS messages. Valid endpoint types are the following: • **gatekeeper**--Endpoint is an H.323 gatekeeper. • **h320-gateway**--Endpoint is an H.320 gateway. • **mcu**--Endpoint is a multipoint control unit (MCU). • **other-gateway**--Endpoint is another type of gateway not specified on this list. • **proxy**--Endpoint is an H.323 proxy. • **terminal**--Endpoint is an H.323 terminal. • **voice-gateway**--Endpoint is a voice gateway.
info -only	Use to indicate to the gatekeeper that messages that meet the specified trigger parameters should be sent to the Gatekeeper Transaction Message Protocol (GKTMP) server application as notifications only and that the gatekeeper should not wait for a response from the GKTMP server application.
shutdown	Use to temporarily disable a trigger. The gatekeeper does not consult triggers in a shutdown state when determining what message to forward to the GKTMP server application.

supported -prefix *value*	Use to send RRQ RAS messages containing a specific supported prefix to the GKTMP server application. • *value* --Value against which to compare the supported prefix in the RAS messages. The possible values are any E.164 pattern used as a gateway technology prefix. The value string can contain any of the following: 0123456789#*.

Command Default

No trigger servers are set.

Command Modes

Gatekeeper configuration (config-gk)

Command History

Release	Modification
12.1(1)T	This command was introduced.
12.2(11)T	This command was implemented on the following platforms: Cisco 2600 series, Cisco 3600 series, Cisco 3700 series, Cisco 7200 series, and Cisco MC3810.

Usage Guidelines

Use this command and its optional submode commands to configure the registration request (RRQ) static server trigger. The gatekeeper checks incoming gateway RRQ messages for the configured trigger information. If an incoming RRQ message contains the specified trigger information, the gatekeeper sends the RRQ message to the GKTMP server application. In addition, the gatekeeper processes the message according to its programmed instructions. If the RRQ message does not contain the specified information, the gatekeeper processes the message but does not send it to the GKTMP server application.

If no submode commands are configured for the RRQ messages, the gatekeeper sends all RRQ messages to the GKTMP server application.

If the gatekeeper receives an RRQ trigger registration message that contains several trigger conditions, the conditions are treated as "OR" conditions. In other words, if an incoming RRQ RAS message meets any one of the conditions, the gatekeeper sends the RAS message to the GKTMP server.

If the gatekeeper receives two RRQ trigger registration messages with the same priority for the same GKTMP server, the gatekeeper retains the second registration and discards the first one. If the gatekeeper receives two RRQ trigger registration messages with different priorities for the same GKTMP server, the gatekeeper checks incoming RRQ messages against the conditions on the higher priority registration before using the lower priority registration. If the gatekeeper receives more than one RRQ trigger registration message with the same priority but for different GKTMP servers, the gatekeepers retains all of the registrations.

The **no** form of the command removes the trigger definition from the Cisco IOS gatekeeper with all statically configured conditions under that trigger.

Examples

The following example configures a trigger registration on gatekeeper "sj.xyz.com" to send all RRQ messages to GKTMP server "Server-123":

```
Router(config-gk)# server trigger rrq sj.xyz.com 1 Server-123 1.14.93.130 1751
Router(config-gk_rrqtrigger)# exit
```

The following example configures an RRQ trigger registration on gatekeeper "alpha", which sends to the GKTMP server "Server-west" any RRQ message containing an MCU endpoint, an H.323 proxy endpoint, or a supported prefix 1#. Other RRQ messages are not sent to the GKTMP server.

```
Router(config-gk)# server trigger rrq alpha 1 Server-west 10.10.10.10 1751
Router(config-gk-rrqtrigger)# endpoint-type mcu
Router(config-gk-rrqtrigger)# endpoint-type proxy
Router(config-gk-rrqtrigger)# supported-prefix 1#
Router(config-gk-rrqtrigger# exit
```

If the RRQ registration message defined above for gatekeeper "alpha" is configured and the gatekeeper receives the following trigger registration:

```
Router(config-gk)# server trigger rrq alpha 2 Server-west 10.10.10.10 1751
Router(config-gk_rrqtrigger)# supported-prefix 1234*
Router(config-gk_rrqtrigger)# exit
```

then gatekeeper "alpha" checks all incoming RRQ messages for the MCU or H.323 proxy endpoint or the supported prefix 1# before checking for the supported prefix 1234*. If any one of those conditions is met, the gatekeeper sends the RRQ message to the GKTMP server "Server-west".

If the second gatekeeper "alpha" RRQ trigger registration had been defined with a priority 1 instead of priority 2, then the second trigger registration would have overridden the first one. In other words, the gatekeeper "alpha" would send to GKTMP server "Server-west" only those RRQ messages that contain a supported prefix of 1234*. All other RRQ messages would not be sent to the GKTMP server.

Related Commands

Command	Description
server registration-port	Configures the server listening port on the gatekeeper.
show gatekeeper servers	Displays the triggers configured on the gatekeeper.

server trigger urq

To configure the unregistration request (URQ) trigger statically on the gatekeeper, use the **server trigger urq**command in gatekeeper configuration mode. Submode commands are available after entering the **server trigger urq**command. To delete a single static trigger on the gatekeeper, use the **no** form of this command. To delete all static triggers on the gatekeeper, use the **all**form of the command.

server trigger urq *gkid priority server-id server-ip-address server-port*
Submode Commands:
info-only
shutdown
endpoint-type *value*
supported-prefix *value*
no server trigger urq *gkid priority server-id server-ip-address server-port*
no server trigger all

Syntax Description

all	Deletes all CLI-configured triggers.
gkid	Local gatekeeper identifier.
priority	Priority for each trigger. Range is from 1 to 20; 1 is the highest priority.
server -id	ID number of the external application.
server -ip-address	IP address of the server.
server -port	Port on which the Cisco IOS gatekeeper listens for messages from the external server connection.

After the command is entered, the software enters a submode that permits you to configure additional filters on the reliability, availability, and serviceability (RAS) message. These filters are optional, and you may configure any of them, one per command line.

endpoint -type *value*	Use to send URQ RAS messages containing a particular endpoint type to the GKTMP server application. • *value* --Value against which to compare the endpoint-type in the RAS messages. Valid endpoint types are the following: • **gatekeeper**--Endpoint is an H.323 gatekeeper. • **h320-gateway**--Endpoint is an H.320 gateway. • **mcu**--Endpoint is a multipoint control unit (MCU). • **other-gateway**--Endpoint is another type of gateway not specified on this list. • **proxy**--Endpoint is an H.323 proxy. • **terminal**--Endpoint is an H.323 terminal. • **voice-gateway**--Endpoint is a voice gateway.

info -only	Use to indicate to the gatekeeper that messages that meet the specified trigger parameters should be sent to the Gatekeeper Transaction Message Protocol (GKTMP) server application as notifications only and that the gatekeeper should not wait for a response from the GKTMP server application.
shutdown	Use to temporarily disable a trigger. The gatekeeper does not consult triggers in a shutdown state when determining what message to forward to the GKTMP server application.
supported -prefix *value*	Use to send URQ RAS messages containing a specific supported prefix to the GKTMP server application. • *value* --Value against which to compare the supported prefix in the RAS messages. The possible values are any E.164 pattern used as a gateway technology prefix. The value string can contain any of the following: 0123456789#*.

Command Default

No trigger servers are set.

Command Modes

Gatekeeper configuration

Command History

Release	Modification
12.1(1)T	This command was introduced.
12.2(11)T	This command was implemented on the following platforms: Cisco 2600 series, Cisco 3600 series, Cisco 3700 series, Cisco 7200 series, and Cisco MC3810.

Usage Guidelines

Use this command and its optional submode commands to configure the unregistration request (URQ) static server trigger. The gatekeeper checks incoming gateway URQ messages for the configured trigger information. If an incoming URQ message contains the specified trigger information, the gatekeeper sends the URQ message to the GKTMP server application. In addition, the gatekeeper processes the message according to its programmed instructions. If the URQ message does not contain the specified information, the gatekeeper processes the message but does not send it to the GKTMP server application.

If no submode commands are configured for the URQ messages, the gatekeeper sends all URQ messages to the GKTMP server application.

If the gatekeeper receives a URQ trigger registration message that contains several trigger conditions, the conditions are treated as "OR" conditions. In other words, if an incoming URQ RAS message meets any one of the conditions, the gatekeeper sends the RAS message to the GKTMP server.

If the gatekeeper receives two URQ trigger registration messages with the same priority for the same GKTMP server, the gatekeeper retains the second registration and discards the first one. If the gatekeeper receives two URQ trigger registration messages with different priorities for the same GKTMP server, the gatekeeper checks incoming URQ messages against the conditions on the higher priority registration before using the lower priority registration. If the gatekeeper receives more than one URQ trigger registration message with the same priority but for different GKTMP servers, the gatekeepers retains all of the registrations.

The the **no** form of the command removes the trigger definition from the Cisco IOS gatekeeper with all statically configured conditions under that trigger.

Examples

The following example configures a trigger registration on gatekeeper "sj.xyz.com" to send all URQ messages to GKTMP server "Server-123":

```
Router(config-gk)# server trigger urq sj.xyz.com 1 Server-123 1.14.93.130 1751
Router(config-gk_urqtrigger)# exit
```

The following example configures a URQ trigger registration on gatekeeper "alpha", which sends to the GKTMP server "Server-west" any URQ message containing an MCU endpoint, an H.323 proxy endpoint, or a supported prefix 1#. Other URQ messages are not sent to the GKTMP server.

```
Router(config-gk)# server trigger urq alpha 1 Server-west 10.10.10.10 1751
Router(config-gk-urqtrigger)# endpoint-type mcu
Router(config-gk-urqtrigger)# endpoint-type proxy
Router(config-gk-urqtrigger)# supported-prefix 1#
Router(config-gk-urqtrigger# exit
```

If the URQ registration message defined above for gatekeeper "alpha" is configured and the gatekeeper receives the following trigger registration:

```
Router(config-gk)# server trigger urq alpha 2 Server-west 10.10.10.10 1751
Router(config-gk_urqtrigger)# supported-prefix 1234*
Router(config-gk_urqtrigger)# exit
```

then gatekeeper "alpha" checks all incoming URQ messages for the MCU or H.323 proxy endpoint or the supported prefix 1# before checking for the supported prefix 1234*. If any one of those conditions is met, the gatekeeper sends the URQ message to the GKTMP server "Server-west".

If the second gatekeeper "alpha" URQ trigger registration had been defined with a priority 1 instead of priority 2, then the second trigger registration would have overridden the first one. In other words, the gatekeeper "alpha" would send to GKTMP server "Server-west" only those URQ messages that contain a supported prefix of 1234*. All other URQ messages would not be sent to the GKTMP server.

Related Commands

Command	Description
server registration-port	Configures the server listening port on the gatekeeper.
show gatekeeper servers	Displays the triggers configured on the gatekeeper.

service

To load and configure a specific, standalone application on a dial peer, use the **service** command in application configuration mode. To remove the application from the dial peer, use the **no** form of this command.

service [**alternate** | **default**] *service-name* *location*
no **service** [**alternate** | **default**] *service-name* *location*

Syntax Description

alternate	(Optional) Alternate service to use if the service that is configured on the dial peer fails.
default	(Optional) Specifies that the default service ("DEFAULT") on the dial peer is used if the alternate service fails.
service-name	Name that identifies the voice application, service, or package. This is a user-defined name and does not have to match the script name.
location	Directory and filename of the Tcl script or VoiceXML document in URL format. For example, the following are valid locations: • built-in applications (builtin:*filename*) • flash memory (flash:filename) • HTTP server (http://../filename) • HTTPS (HTTP over Secure Socket Layer (SSL)) server (https://../filename) • TFTP server (tftp://../filename)

Command Default

The default service ("DEFAULT") is used if no other services are configured.

Command Modes

Application configuration (config-app)

Command History

Release	Modification
Cisco IOS XE 26.2.1	This command was modified to display warning message for insecure protocol usage.
12.4(15)T	The *location* argument was modified to accept an HTTPS server URL. The description of the *location* argument was modified to describe how to specify the location for built-in applications.
12.3(14)T	This command was introduced.

Usage Guidelines

Use this command to load a service on the gateway. A service is a standalone application, such as a VoiceXML document or a Tcl script.

Warning Starting with Cisco IOS XE 26.2.1, a warning message is displayed when insecure protocols such as HTTP, FTP, or TFTP are used, as they do not provide encryption or authentication. Use secure alternatives such as HTTPS, SFTP, or SCP instead.

Examples

The following example shows a debit application configured on the dial peer using insecure HTTP protocol displays a warning message:

```
Device(config)#application
Device(config-app)#service debit http://10.10.10.70//tftpboot/COLT-DE-CUCM.cfg
SECURITY WARNING - Module: CONFIG_VOICE, Command: service debit
http://10.10.10.70//tftpboot/COLT-DE-CUCM.cfg,
Reason: Legacy protocol poses data confidentiality and integrity risks due to lack of
encryption and authentication,
Description: service debitcard configured with FTP/HTTP/TFTP URL protocol,
Remediation: Use secure protocols such as HTTPS, SFTP, or SCP instead of insecure HTTP,
FTP, or TFTP
Device(config-app-param)#
```

Examples

The following example shows a debitcard application configured on the dial peer.

```
Router(config)# application
Router(config-app)# service debitcard
tftp://server-1//tftpboot/scripts/app_debitcard.2.0.2.8.tcl
```

The following example shows the VoiceXML application myapp located on an HTTPS server configured on the dial peer.

```
Router(config)# application
Router(config-app)# service myapp https://myserver/myfile.vxml
```

The following example shows the auto-attendant (AA) service, called aa, which is a Tcl script embedded in the Cisco IOS software.

```
Router(config)# application
Router(config-app)# service queue builtin:app-b-acd
```

Related Commands

Command	Description
application (application configuration)	Configures an application on a dial peer.
call application alternate	Specifies an alternate application to use if the application that is configured in the dial peer fails.
call application voice	Defines the name of a voice application and specifies the location of the Tcl or VoiceXML document to load for this application.

service dsapp

To configure supplementary IP Centrex-like services for FXS phones on voice gateways to interwork with SIP-based softswitches, use the **service dsapp**command in the gateway-application configuration mode. Hookflash triggers a supplementary feature based on the current state of the call. To reset to the defaults, use the **no** form of this command.

service dsapp [*paramspace* **dialpeer** *dial-peer tag*] [*paramspace* **disc-toggle-time** *seconds*] [*paramspace* **callWaiting** *TRUEFALSE*] [*paramspace* **callConference** *TRUEFALSE*] [*paramspace* **blind-xfer-wait-time** *seconds*] [*paramspace* **callTransfer** *TRUEFALSE*]
no service dsapp

Syntax Description

paramspace	Defines a package or service on the gateway, the parameters in that package or service become available for configuration when you use this argument.
dialpeer *dial-peer tag*	(Optional) Specifies the fixed dialpeer used to setup the call to the SIP server (trunk) side.
disc-toggle-time *seconds*	(Optional) Specifies the seconds to wait before switching to a call on hold if the active call disconnects. You can specify a range between 10 and 30 seconds.
callWaiting *TRUE* | *FALSE*	Toggles support for call waiting.
callConference *TRUE* | *FALSE*	Toggles support for call conferencing used to establish two calls with a single connection such that all three parties can talk together.
blind-xfer-wait-time *seconds*	Specifies the seconds to wait before triggering a blind call transfer. You can specify a range between 0 and 10 seconds. If you specify 0 seconds, no blind transfer call occurs.
callTransfer *TRUE* | *FALSE*	Toggles support for call transfers.

Command Default

If no supplementary features are defined, the defaults are as follows:

- **dialpeer** : -1
- **disc-toggle-time** : 10 seconds
- **callWaiting** : TRUE (enabled)
- **callConference** : TRUE (enabled)
- **blind-xfer-wait-time** : 0 seconds
- **callTransfer** : TRUE (enabled)

Command Modes

Gateway-application configuration (config-app-param)

Command History

Release	Modification
12.4(11)T	This command was introduced.

Usage Guidelines

Use the **service dsapp**command to configure supplementary Centrex-like features on FXS phones to interwork with SIP-based softswitches. Hookflash triggers supplementary features based on the current state of the call:

- Call Hold
- Call Waiting
- Call Transfer
- 3-Way Conference

Call Hold

Allows a call to be placed in a non-active state (with no media exchange). The table below summarizes the hookflash feature support for Call Hold.

Table 1: Call Hold Hookflash Services

State	Action	Result	Response to FXS Line
Active call	Hookflash	Held call for remote party.	Second dial tone for FXS phone.
Call on hold	Hookflash	Active call.	FXS line connects to call.
Call on hold and active call	Hookflash	Active and held calls are swapped.	FXS line connects to previous held call.
	On hook	Active call is dropped.	Reminder ring on FXS line.
	Call on hold goes on hook	Call on hold is dropped.	None.
	Active call goes on hook	Active call is dropped	Silence.

Call Waiting

Allows a second call to be received while the phone is active with a call. The table below summarizes the hookflash feature support for Call Waiting.

Table 2: Call Waiting Hookflash Services

State	Action	Result	Response to FXS Line
Active call and waiting call	Hookflash.	Swap active call and waiting call.	FXS line connects to waiting call.
	Active call goes on hook.	Active call is disconnected.	Silence.
	Waiting call goes on hook.	Stay connected to active call.	None.
	On hook.	Active call is dropped.	Reminder ring on FXS line.

Call Transfer

With call transfer, you can do the following:

- Put an active call on hold while establishing a second call.
- Set up a call between two users
- Transfer calls by using these options
  - -Blind transfer
  - Semi-attended transfer
  - Attended transfer

The table below summarizes the hookflash feature support for Call Transfer.

Table 3: Call Transfer Hookflash Services

State	Action	Result	Response to FXS Line
Active call	Hookflash.	Call is placed on hold.	Second dial tone.
Call on hold and outgoing dialed or alerting or active call	On hook.	Call on hold and active call.	
Call on hold and outgoing active call	Active call goes on hook.	Held call remains; active call dropped.	Silence.
Call on hold and outgoing active call	Call on hold goes on hook.	Active call remains; call on hold dropped.	None.
Call on hold and outgoing alerting call	Hookflash.	Active call dropped.	FXS line connects to previous held call.

3-Way Conference

Establishes two calls with a single connection, so that three parties can talk together. The table below summarizes the hookflash feature support for 3-way conferencing.

Table 4: 3-Way Conference Hookflash Services

State	Action	Result	Response to FXS Line
Active call	Hookflash	Call on hold.	Second dial tone.
Call on hold and active call		Join call on hold and active call.	Media mixing of both calls.

Examples

Enabling the DSApp Service

You can configure DSApp services either to a specific dial-peer, or globally to all dial peers. The following example shows the configuration to enable DSApp on a specific dial peer:

```
Gateway#
```

```
configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Gateway(conf)#

application
Gateway(conf-app)#

dial-peer voice 1000 pots
Gateway(config-app)#
service dsapp
```

The following example shows the configuration to enable DSApp globally on all dial peers:

```
Gateway#

configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Gateway(conf)#

application
Gateway(config-app)# global
Gateway(config-app-global)#
service default dsapp
```

Configuring Call Hold

The following example shows the configuration to enable the Call Hold feature:

```
Gateway#

configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Gateway(conf)#

application
Gateway(config-app)#
service dsapp
Gateway
(config-app-param)#
param callHold TRUE
```

Configuring Call Waiting

The following example shows the configuration to enable the Call Waiting feature:

```
Gateway#

configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Gateway(conf)#

application
Gateway(config-app)#
service

dsapp
Gateway
```

```
(config-app-param)#
param callWaiting TRUE
```

Configuring Call Transfer

The following example shows the configuration to enable the Call Transfer feature:

```
Gateway#

configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Gateway(conf)#

application
Gateway(config-app)#
service dsapp
Gateway
(config-app-param)#
param callTransfer TRUE
```

Configuring 3-Way Conferencing

The following example shows the configuration to enable the 3-Way Conferencing feature:

```
Gateway#

configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Gateway(conf)#

application
Gateway(config-app)#
service dsapp
Gateway
(config-app-param)#
param callConference TRUE
```

Configuring Disconnect Toggle Time

In this example, a disconnect toggle time is configured that specifies the amount of time in seconds the system should wait before committing the call transfer after the originating call is placed on hook.

```
Gateway#
configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Gateway(conf)#
application
Gateway(config-app)#
service dsapp
Gateway(config-app-param)#
param disc-toggle-time 10
```

Configuring Blind Transfer Wait Time

In this example, a blind transfer call wait time is configured that specifies the amount of time in seconds the system should wait before committing the call transfer, after the originating call is placed on hook.

```
Gateway#
configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Gateway(conf)#
application
Gateway(config-app)#
service dsapp
Gateway(config-app-param)#
param blind-xfer-wait-time 10
```

Configuring a Fixed Dial Peer Used for Outgoing Calls on SIP Trunk Side

In this example, a fixed dial peer is configured to set up a call to the SIP server (trunk) side.

```
Gateway#
configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Gateway(conf)#
application
Gateway(config-app)#
service dsapp
Gateway(config-app-param)#
param dialpeer 5000
```

Related Commands

Command	Description
offer call-hold	Specifies the method of call hold on the gateway.

service-flow primary upstream

To assign a quality of service (QoS) policy to the data traveling between the cable modem and the multiple service operator (MSO) cable modem termination system (CMTS), use the **service-flow primary upstream** command in interface configuration mode. To disable the QoS policy, use the **no** form of this command.

service-flow primary upstream
no service-flow primary upstream

Syntax Description

This command has no arguments or keywords.

Command Default

This command is disabled by default.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.4(11)T	This command was introduced.

Usage Guidelines

This command is supported in the upstream direction only. Service flows are unidirectional.

Examples

The following example assigns a QoS policy to the data traveling between the cable modem and the MSO CMTS:

```
Router# configure terminal
Router(config)# interface Cable-Modem 0/2/0

Router(config-if)# service-flow primary upstream
```

service-map

To configure the HTTP application service map for the phone proxy instance, use the **service-map** command in phone proxy configuration mode. To remove the HTTP application service map, use the **no** form of the command.

service-map server-addr ipv4 *http-ipv4-address* **port** *http-server-port-number* **acc-addr ipv4** *access-ipv4-address***port** *access-port-number*
no service-map server-addr ipv4 *http-ipv4-address* **port** *http-server-port-number* **acc-addr ipv4** *access-ipv4-address***port** *access-port-number*

Syntax Description

http-ipv4-address	Specifies the IPv4 address of the HTTP server.
port *http-server-port-number*	The port number of the HTTP server. The range is 1 to 65535.
acc-addr ipv4 *access-ipv4-address*	Specifies the IPv4 address of the access side server.
port *access-port-number*	The port number of the access side server. The range is 1 to 65535.

Command Default

No HTTP application service map is configured.

Command Modes

Phone proxy configuration mode (config-phone-proxy)

Command History

Release	Modification
15.3(3)M	This command was introduced.

Usage Guidelines

Example

The following example shows how to configure an HTTP application service map for the phone proxy instance called “first-pp”:

```
Device(config)# voice-phone-proxy first-pp
Device(config-phone-proxy)# service-map server-addr ipv4 192.0.2.50 port 8080 acc-addr ipv4
 10.0.0.8 port 1234
```

service-relationship

To enter Annex G neighbor configuration mode and enable service relationships for the particular neighbor, use the **service-relationship** command in Annex G neighbor configuration mode. To exit this mode, use the **no** form of this command.

service-relationship
no service-relationship

Syntax Description

This command has no arguments or keywords.

Command Default

Disabled

Command Modes

Annex G neighbor configuration (config-annexg-neigh)

Command History

Release	Modification
12.2 (11)T	This command was introduced.

Usage Guidelines

Service relationships are defined to be unidirectional. If a service relationship is established between border element A and border element B, A is entitled to send requests to B and to expect responses. For B to send requests to A and to expect responses, a second service relationship must be established. Repeat this command for each border-element neighbor that you configure.

Note The **no shutdown** command must be used to enable each service relationship.

Examples

The following example enables a service relationship on a border element:

```
Router(config-annexg-neigh)# service-relationship
```

Related Commands

Command	Description
access -policy	Requires that a neighbor be explicitly configured.
inbound ttl	Sets the inbound time-to-live value.
outbound retry -interval	Defines the retry period for attempting to establish the outbound relationship between border elements.
retry interval	Defines the time between delivery attempts.
retry window	Defines the total time for which a border element attempts delivery.
shutdown	Enables or disables the border element.

service-type call-check

To identify preauthentication requests to the authentication, authorization, and accounting (AAA) server, use the **service-type call-check** command in AAA preauthentication configuration mode. To return this setting to the default, use the **no** form of this command.

service-type call-check
no service-type call-check

Syntax Description

This command has no arguments or keywords.

Command Default

The service type is not set to call-check.

Command Modes

AAA preauthentication configuration (config-preauth)

Command History

Release	Modification
12.2(11)T	This command was introduced.

Usage Guidelines

Setting the service-type attribute to call-check causes preauthentication access requests to include this value, which allows AAA servers to distinguish preauthentication requests from other types of Access-Requests. This command has no effect on packets that are not of the preauthentication type.

Examples

The following example sets the RADIUS service-type attribute to call-check:

```
Router(config)# aaa preauth
Router(config-preauth)# service-type call-check
```

Related Commands

Command	Description
aaa preauth	Enters AAA preauthentication configuration mode.



session through sgcp tse payload

- session, on page 95
- session group, on page 96
- session protocol (dial peer), on page 97
- session protocol (Voice over Frame Relay), on page 99
- session protocol aal2, on page 101
- session protocol multicast, on page 102
- session refresh, on page 103
- session start, on page 104
- session target (MMoIP dial peer), on page 106
- session target (POTS dial peer), on page 109
- session target (VoATM dial peer), on page 110
- session target (VoFR dial peer), on page 113
- session target (VoIP dial peer), on page 115
- session target, on page 120
- session transport, on page 121
- session transport (H.323 voice-service), on page 123
- session transport (SIP), on page 124
- session-set, on page 126
- session-timeout, on page 127
- set, on page 128
- set http client cache stale, on page 130
- set pstn-cause, on page 131
- set sip-status, on page 134
- settle-call, on page 137
- settlement, on page 138
- settlement roam-pattern, on page 140
- sgcp, on page 141
- sgcp call-agent, on page 143
- sgcp graceful-shutdown, on page 145
- sgcp max-waiting-delay, on page 147
- sgcp modem passthru, on page 149
- sgcp quarantine-buffer disable, on page 151
- sgcp request retries, on page 153

- sgcp request timeout, on page 155
- sgcp restart, on page 157
- sgcp retransmit timer, on page 159
- sgcp timer, on page 161
- sgcp tse payload, on page 163
- source filter, on page 165

session

To associate a transport session with a specified session group, use the **session** command in backhaul session manager configuration mode. To delete the session, use the **no** form of this command.

session group *group-name remote-ip remote-port local-ip local-port priority*
no session group *group-name remote-ip remote-port local-ip local-port priority*

Syntax Description

group -name	Session-group name.
remote -ip	Remote IP address.
remote -port	Remote port number. Range is from 1024 to 9999.
local -ip	Local IP address.
local -port	Local port number. Range is from 1024 to 9999.
priority	Priority of the session-group. Range is from 0 to 9999; 0 is the highest priority.

Command Default

No default behavior or values

Command Modes

Backhaul session manager configuration

Command History

Release	Modification
12.1(1)T	This command was introduced.
12.2(4)T	This command was implemented on the following platforms: Cisco 2600 series, Cisco 3600 series, and Cisco MC3810.
12.2(2)XB	This command was implemented on the Cisco AS5350 and Cisco AS5400.
12.2(2)XB1	This command was implemented on the Cisco AS5850.
12.2(8)T	This command was implemented on the Cisco IAD2420 series. Support for the Cisco AS5350, Cisco AS5400, and Cisco AS5850 is not included in this release.
12.2(11)T	This command is supported on the Cisco AS5350, Cisco AS5400, and Cisco AS5850 in this release.

Usage Guidelines

It is assumed that the server is located on a remote machine.

Examples

The following example associates a transport session with the session group "group5" and specifies the parameters:

```
Router(config-bsm)# session group
 group5
 172.13.2.72 5555 172.18.72.198 5555 1
```

session group

To associate a transport session with a specified session group, use the **session group**command in backhaul session-manager configuration mode. To delete the session, use the **no** form of this command.

session group *group-name remote-ip remote-port local-ip local-port priority*
no session group *group-name remote-ip remote-port local-ip local-port priority*

Syntax Description

group -name	Session-group name.
remote -ip	Remote IP address.
remote -port	Remote port number. Range is from 1024 to 9999.
local -ip	Local IP address.
local -port	Local port number. Range is from 1024 to 9999.
priority	Priority of the session group. Range is from 0 to 9999; 0 has the highest priority.

Command Default

No default behavior or values.

Command Modes

Backhaul session-manager configuration

Command History

Release	Modification
12.1(1)T	This command was introduced.
12.2(2)T	This command was implemented on the Cisco 7200 series.
12.2(4)T	This command was implemented on the following platforms: Cisco 2600 series, Cisco 3600 series, and Cisco MC3810.
12.2(2)XB1	This command was implemented on the Cisco AS5850.
12.2(8)T	This command was implemented on the Cisco IAD2420 series.

Usage Guidelines

The server is assumed to be located on a remote machine.

Examples

The following example associates a transport session with the session group named "group5" and specifies the keywords described above:

```
session group
 group5
 172.16.2.72 5555 192.168.72.198 5555 1
```

session protocol (dial peer)

To specify a session protocol for calls between local and remote routers using the packet network, use the **session protocol** command in dial-peer configuration mode. To reset to the default, use the **no** form of this command.

session protocol {**aal2-trunk** | **cisco** | **sipv2** | **smtp**}
no session protocol

Syntax Description

aal2 -trunk	Dial peer uses ATM adaptation layer 2 (AAL2) nonswitched trunk session protocol.
cisco	Dial peer uses the proprietary Cisco VoIP session protocol.
sipv2	Dial peer uses the Internet Engineering Task Force (IETF) Session Initiation Protocol (SIP). Use this keyword with the SIP option.
smtp	Dial peer uses Simple Mail Transfer Protocol (SMTP) session protocol.

Command Default

No default behaviors or values

Command Modes

Dial-peer configuration (config-dial-peer)

Command History

Release	Modification
11.3(1)T	This command was introduced for VoIP peers on the Cisco 3600 series.
12.0(3)XG	This command was modified to support VoFR) dial peers.
12.0(4)XJ	This command was modified for store-and-forward fax on the Cisco AS5300.
12.1(1)XA	This command was implemented for VoATM dial peers on the Cisco MC3810. The **aal2-trunk** keyword was added.
12.1(1)T	This command was integrated into Cisco IOS Release 12.1(1)T. The **sipv2** keyword was added.
12.1(2)T	This command was integrated into Cisco IOS Release 12.1(2)T.
12.2(2)T	This command was implemented on the Cisco 7200 series.
12.2(4)T	This command was implemented on the Cisco 1750.
12.2(2)XA	This command was implemented on the Cisco AS5350 and Cisco AS5400.
12.2(2)XB1	This command was implemented on the Cisco AS5850.

Release	Modification
12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T and was implemented on the Cisco 7200 series. Support for the Cisco AS5300, Cisco AS5350, Cisco AS5400, and Cisco AS5850 is not included in this release. The **aal2-trunk** and **smtp** keywords are not supported on the Cisco 7200 series in this release.
12.2(11)T	This command is supported on the Cisco AS5350, Cisco AS5400, and Cisco AS5850 in this release.
Cisco IOS XE Amsterdam 17.2.1r	Introduced support for YANG models.

Usage Guidelines

The **cisco**keyword is applicable only to VoIP on the Cisco 1750, Cisco 1751, Cisco 3600 series, and Cisco 7200 series routers.

The **aal2-trunk** keyword is applicable only to VoATM on the Cisco 7200 series router.

This command applies to both on-ramp and off-ramp store-and-forward fax functions.

Examples

The following example shows that AAL2 trunking has been configured as the session protocol:

```
dial-peer voice 10 voatm
 session protocol aal2-trunk
```

The following example shows that Cisco session protocol has been configured as the session protocol:

```
dial-peer voice 20 voip
 session protocol cisco
```

The following example shows that a VoIP dial peer for SIP has been configured as the session protocol for VoIP call signaling:

```
dial-peer voice 102 voip
 session protocol sipv2
```

Related Commands

Command	Description
dial-peer voice	Enters dial-peer configuration mode and specifies the method of voice-related encapsulation.
session target (VoIP)	Configures a network-specific address for a dial peer.

session protocol (Voice over Frame Relay)

To establish a Voice over Frame Relay protocol for calls between the local and remote routers via the packet network, use the **session protocol** command in dial-peer configuration mode. To reset to the default, use the **no** form of this command.

session protocol {**cisco-switched** | **frf11-trunk**}
no session protocol

Syntax Description

cisco -switched	Proprietary Cisco VoFR session protocol. (This is the only valid session protocol for the Cisco 7200 series.)
frf11 -trunk	FRF.11 session protocol.

Command Default

cisco-switched

Command Modes

Dial-peer configuration (config-dial-peer)

Command History

Release	Modification
11.3(1)T	This command was introduced for VoIP.
12.0(3)XG	This command was modified to support VoFR on the following platforms: Cisco 2600 series, Cisco 3600 series, Cisco 7200 series, and Cisco MC3810.
12.0(4)T	The **cisco-switched** and **frf11-trunk** keywords were added for VoFR dial peers.

Usage Guidelines

For Cisco-to-Cisco dial peer connections, Cisco recommends that you use the default session protocol because of the advantages it offers over a pure FRF.11 implementation. When connecting to FRF.11-compliant equipment from other vendors, use the FRF.11session protocol.

Note When using the FRF.11 session protocol, you must also use the **called-number** command.

Examples

The following example configures the FRF.11 session protocol for VoFR dial peer 200:

```
dial-peer voice 200 vofr
 session protocol frf11-trunk
 called-number 5552150
```

Related Commands

Command	Description
called-number (dial-peer)	Enables an incoming VoFR call leg to get bridged to the correct POTS call leg when using a static FRF.11 trunk connection.

Command	Description
codec (dial-peer)	Specifies the voice coder rate of speech for a Voice over Frame Relay dial peer.
cptone	Specifies a regional analog voice interface-related tone, ring, and cadence setting.
destination-pattern	Specifies either the prefix, the full E.164 telephone number, or an ISDN directory number (depending on the dial plan) to be used for a dial peer.
dtmf-relay (Voice over Frame Relay)	Enables the generation of FRF.11 Annex A frames for a dial peer.
preference	Indicates the preferred order of a dial peer within a rotary hunt group.
session target	Specifies a network-specific address for a specified dial peer or destination gatekeeper.
signal-type	Sets the signaling type to be used when connecting to a dial peer.

session protocol aal2

To enter voice-service-session configuration mode and specify ATM adaptation layer 2 (AAL2) trunking, use the **session protocol aal2**command in voice-service configuration mode.

session protocol aal2

Syntax Description

This command has no arguments or keywords.

Command Default

No default behavior or values.

Command Modes

Voice-service configuration (config-voi-serv)

Command History

Release	Modification
12.1(1)XA	This command was introduced on the Cisco MC3810.
12.1(2)T	This command was integrated into Cisco IOS Release 12.1(2)T.
12.2(2)T	This command was implemented on the Cisco 7200 series.

Usage Guidelines

This command applies to VoATM on theCisco 7200 series router.

In the voice-service-session configuration mode for AAL2, you can configure only AAL2 features, such as call admission control and subcell multiplexing.

Examples

The following example accesses voice-service-session configuration mode, beginning in global configuration mode:

```
voice service voatm
 session protocol aal2
```

session protocol multicast

To set the session protocol as multicast, use the **session protocol multicast** command in dial-peer configuration mode. To reset to the default protocol, use the **no** version of this command.

session protocol multicast
no session protocol multicast

Syntax Description

This command has no arguments or keywords.

Command Default

Default session protocol: Cisco.

Command Modes

Dial-peer configuration (config-dial-peer)

Command History

Release	Modification
12.1(2)XH	This command was introduced for the Cisco Hoot and Holler over IP application on the Cisco 2600 series and Cisco 3600 series.
12.1(3)T	This command was integrated into Cisco IOS Release 12.1(3)T.
12.2(8)T	This command was implemented on the Cisco 1750 and Cisco 1751.

Usage Guidelines

Use this command for voice conferencing in a hoot and holler networking implementation. This command allows more than two ports to join the same session simultaneously.

Examples

The following example shows the use of the **session protocol multicast** dial-peer configuration command in context with its accompanying commands:

```
dial-peer voice 111 voip
 destination-pattern 111
 session protocol multicast
 session target ipv4:237.111.0.111:22222
 ip precedence 5
 codec g711ulaw
```

Related Commands

Command	Description
session target ipv4	Assigns the session target for voice-multicasting dial peers.

session refresh

To enable SIP session refresh globally, use the **session refresh**command in SIP configuration mode. To disable the session refresh, use the **no** form of this command.

session refresh
no session refresh

Syntax Description

This command has no arguments or keywords.

Command Default

No session refresh

Command Modes

SIP configuration (conf-serv-sip)

Command History

Release	Modification
15.1(2)T	This command was introduced.
Cisco IOS XE Cupertino 17.7.1a	Introduced support for YANG models.

Usage Guidelines

Use the SIP **session refresh**command to send the session refresh request.

Examples

The following example sets the session refresh under SIP configuration mode:

```
Router(conf-serv-sip)# Session refresh
```

Related Commands

Command	Description
voice-class sip session refresh	Enables session refresh at dial-peer level.

session start

To start a new instance (session) of a Tcl IVR 2.0 application, use the **session start** command in application configuration mode. To stop the session and remove the configuration, use the **no** form of this command.

session start *instance-name application-name*
no session start *instance-name*

Syntax Description

instance-name	Alphanumeric label that uniquely identifies this application instance.
application-name	Name of the Tcl application. This is the name of the application that was assigned with the **service** command.

Command Default

No default behavior or values

Command Modes

Application configuration

Command History

Release	Modification
12.3(14)T	This command was introduced to replace the **call application session start** (global configuration) command.

Usage Guidelines

- This command starts a new session, or instance, of a Tcl IVR 2.0 application. It cannot start a session for a VoiceXML application because Cisco IOS software cannot start a VoiceXML application without an active call leg.
- You can start an application instance only after the Tcl application is loaded onto the gateway with the **service** command.
- If this command is used, the session restarts if the gateway reboots.
- If the application session stops running, it does not restart unless the gateway reboots. A Tcl script might intentionally stop running by executing a "call close" command for example, or it might fail because of a script error.
- You can start multiple instances of the same application by using different instance names.

Examples

The following example starts a session named my_instance for the application named demo:

```
application
session start my_instance demo
```

The following example starts another session for the application named demo:

```
application
session start my_instance2 demo
```

Related Commands

Command	Description
call application session start (global configuration)	Starts a new instance (session) of a Tcl IVR 2.0 application.
service	Loads a specific, standalone application on a dial peer.
show call application services registry	Displays a one-line summary of all registered services.
show call application sessions	Displays summary or detailed information about voice application sessions.

session target (MMoIP dial peer)

To designate an e-mail address to receive T.37 store-and-forward fax calls from a Multimedia Mail over IP (MMoIP) dial peer, use the **session target**command indial peer configuration mode. To remove the target address, use the **no** form of this command.

session target mailto: {*name* | **d** | **m** | **e**} [**@***domain-name*]
no session target

Syntax Description

mailto:	Matching calls are passed to the network using Simple Mail Transfer Protocol (SMTP) or Extended Simple Mail Transfer Protocol (ESMTP).
name	String that can be an e-mail address, name, or mailing list alias.
d	Macro that is replaced by the destination pattern of the gateway access number, which is the called number or dialed number identification service (DNIS) number.
m	Macro that is replaced by the redirecting dialed number (RDNIS) if present; otherwise, it is replaced by the gateway access number (DNIS). This macro requires use of the fax detection interactive voice response (IVR) application. **Note** Other strings can be passed to mailto in place of **m** if you modify the fax detection application Tool Command Language (Tcl) script or VoiceXML document. For more information, see to the readme file that came with the Tcl script or the *Cisco VoiceXML Programmer's Guide.*
e	Macro that is replaced by the DNIS, the RDNIS, or a string that represents a valid e-mail address, as specified by the *cisco-mailtoaddress* variable in the transfer tag of the VoiceXML fax detection document. By default, if the *cisco-mailtoaddress* variable is not specified in the fax detection document, the DNIS is mapped to **e**. If **e** is not specified for the **session target mailto** command in the MMoIP dial peer, but the *cisco-mailtoaddres* s variable is specified in the transfer tag of the fax detection document, then whatever is specified in the MMoIP dial peer takes precedence; the *cisco-mailtoaddress* variable is ignored. **Note** If a domain name is configured with this command, the VoiceXML document should pass only the username portion of the e-mail address and not the domain. If the domain name is passed from *cisco-mailtoaddress,* the **session target mailto** command should specify only **e**.
@ *domain-name*	(Optional) String that contains the domain name to be associated with the target address, preceded by the at sign (@); for example, *@mycompany.com* .

Command Default

No default behavior or values

Command Modes

Dial peer configuration (config-dial-peer)

Command History

Release	Modification
11.3(1)T	This command was introduced.
12.0(4)T	This command was modified to support store-and-forward fax.
12.1(5)XM1	The **m**keyword was introduced for the fax detection feature on the Cisco AS5300.
12.2(2)XA	This command was implemented on the Cisco AS5350 and Cisco AS5400.
12.2(2)XB	The **e**keyword was introduced for VoiceXML fax detection on the Cisco AS5300.
12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T and was implemented on the following platforms: Cisco 1751, Cisco 2600 series, Cisco 3600 series, Cisco 3725, and Cisco 3745.
12.2(11)T	This command was implemented on the following platforms: Cisco AS5300, Cisco AS5350, and Cisco AS5400.

Usage Guidelines

Use this command to deliver e-mail to one recipient by specifying one e-mail name, or to deliver e-mail to multiple recipients by specifying an e-mail alias as the *name* argument and having that alias expanded by the mailer.

Use the **m** macro to include the redirecting dialed number (RDNIS) as part of the e-mail name when using the fax detection IVR application. If **m** is specified and RDNIS is not present in the call information, the access number of the gateway (the dialed number, or DNIS) is used instead. For example, if the calling party originally dialed 6015550111 to send a fax, and the call was redirected (forwarded on busy or no answer) to 6015550122 (the gateway), the RDNIS is 6015550111, and the DNIS is 6015550122.

Use the **e** macro to map the *cisco-mailtoaddress* variable in the VoiceXML fax detection document to the username portion of the e-mail address when sending a fax. If the VoiceXML document does not specify the *cisco-mailtoaddress* variable in the transfer tag, the application maps the DNIS to the e-mail address username.

Examples

The following example delivers fax-mail to multiple recipients:

```
dial-peer voice 10 mmoip
 session target mailto:marketing-information@mailer.example.com
```

Assuming that mailer.example.com is running the sendmail application, you can put the following information into its /etc/aliases file:

```
marketing-information:
 john@example.com,
 fax=+14085550112@sj-offramp.example.com
```

The following example uses the fax detection IVR application. Here, the **session target (MMoIP dial peer)**commandforwards fax calls to an e-mail account that uses the Redirected Dialed Number Identification Service (RDNIS) as part of its address. In this example, the calling party originally dialed 6015550111 to send a fax, and the call was forwarded (on busy or no answer) to 6015550122, which is the incoming number for the gateway being configured. The RDNIS is 6015550111, and the dialed number (DNIS) is 6015550122. When faxes are forwarded from the gateway, the session target in the example is expanded to 6015550111@mail-server.unified-messages.com.

```
dial-peer voice 4 mmoip
 session target mailto:$m$@mail-server.unified-messages.com
```

The following examples configure a session target for a VoiceXML fax detection application. In this example, the VoiceXML document passes just the username portion of the e-mail address, for example, "johnd":

```
dial-peer voice 4 mmoip
 session target mailto:$e$@cisco.com
```

In this example, the VoiceXML document passes the complete e-mail address including domain name, for example, "johnd@cisco.com":

```
dial-peer voice 5 mmoip
 session target mailto:$e$
```

Related Commands

Command	Description
destination-pattern	Specifies either the partial or full E.164 telephone number (depending on your dial plan) used to match the dial peer.
dial-peer voice	Enters dial-peer configuration mode and defines a dial peer.

session target (POTS dial peer)

To designate loopback calls from a POTS dial peer, use the **session target** command in dial-peer configuration mode. To reset to the default, use the **no** form of this command.

session target {**loopback:compressed** | **loopback:uncompressed**}
no session target

Syntax Description

loopback:compressed	All voice data is looped back in compressed mode to the source.
loopback:uncompressed	All voice data is looped back in uncompressed mode to the source.

Command Default

No loopback calls are designated.

Command Modes

Dial-peer configuration (config-dial-peer)

Command History

Release	Modification
11.3(1)T	This command was introduced on the Cisco 2600 series and Cisco 3600 series.
12.0(3)T	This command was implemented on the Cisco AS5300.
12.2(2)XA	This command was implemented on the Cisco AS5350 and Cisco AS5400.
12.2(2)XB1	This command was implemented on the Cisco AS5850.
12.2(8)T	Support for the Cisco AS5300, Cisco AS5350, Cisco AS5400, and Cisco AS5850 is not included in this release.
12.2(11)T	This command was integrated into Cisco IOS Release 12.2(11)T and is supported on the Cisco AS5200, Cisco AS5350, Cisco AS5400, and Cisco AS5850 in this release.

Usage Guidelines

Use this command to test the voice transmission path of a call. The loopback point depends on the call origin and the loopback type selected.

Examples

The following example loops back the traffic from the dial peer in compressed mode:

```
dial-peer voice 10 pots
 session target loopback:compressed
```

Related Commands

Command	Description
dial -peer voice	Enters dial-peer configuration mode and specifies the method of voice-related encapsulation.

session target (VoATM dial peer)

To specify a network-specific address for a specified VoATM dial peer, use the **session target** command in dial-peer configuration mode. To reset to the default, use the **no** form of this command.

Cisco 3600 Series Routers
session target *interface* **pvc** {*name* | *vpi*/*vcivci*}
no session target

Cisco 7200 Series Routers
session target atm *slot*/*port* **pvc** {*word* | *vpi*/*vcivci*} *cid*
no session target

Syntax Description

serial	Serial interface for the dial-peer address.
atm	ATM interface. The only valid number is 0.
interface	Interface type and interface number on the router.
slot / *port*	Slot and port numbers for the dial-peer address.
pvc	Specific ATM permanent virtual circuit (PVC) for this dial peer.
name	PVC name.
word	(Optional) Name that identifies the PVC. The argument can identify the PVC if a word identifier was assigned when the PVC was created.
vpi / *vci*	ATM network virtual path identifier (VPI) and virtual channel identifier (VCI) of this PVC. Values are as follows: • Cisco 3600 series with Multiport T1/E1 ATM network module with inverse multiplexing over ATM (IMA): *vpi*range is from 0 to 5; *vci* range is from 1 to 255. • OC3 ATM network module: *vpi* range is from 0 to 15; *vci* range is from 1 to 1023.
vci	ATM network virtual channel identifier (VCI) of this PVC.
cid	ATM network channel identifier (CID) of this PVC. Range is from 8 to 255.

Command Default

Command is enabled with no IP address or domain name defined.

Command Modes

Dial-peer configuration (config-dial-peer)

Command History

Release	Modification
11.3(1)T	This command was introduced.
11.3(1)MA	This command was modified to support VoATM, VoHDLC, and POTS dial peers. The command was implemented on the Cisco MC3810.

Release	Modification
12.0(3)XG	This command was modified to support VoFR dial peers. The command was implemented on the Cisco 2600 series and Cisco 3600 series.
12.0(4)T	This command was integrated into Cisco IOS Release 12.0(4)T.
12.0(7)XK	This command was modified to support VoATM and VoIP dial peers. The command was implemented on the Cisco 3600 series and the Cisco MC3810. Support for VoHDLC was removed.
12.1(1)XA	This command was modified to provide enhanced support for VoATM dial peers.
12.1(2)T	This command was integrated into Cisco IOS Release 12.1(2)T.
12.2(2)T	This command was implemented on the Cisco 7200 series.

Usage Guidelines

Use the **session target**command to specify a network-specific address or domain name for a dial peer. Whether you select a network-specific address or a domain name depends on the session protocol that you select. The syntax of this command complies with the simple syntax of mailto: as described in RFC 1738.

Use the **session target loopback** command to test the voice transmission path of a call. The loopback point depends on the call origin and the loopback type selected.

This command applies to on-ramp store-and-forward fax functions.

You must enter the session protocol aal2-trunk dial-peer configuration command before you can specify a CID for a dial peer for VoATM on the Cisco 7200 series router.



Note This command does not apply to POTS dial peers.

Examples

The following example configures a session target for VoATM. The session target is sent to ATM interface 0 for a PVC with a VCI of 20.

```
dial-peer voice 12 voatm
 destination-pattern 13102221111
 session target atm0 pvc 20
```

The following example delivers fax-mail to multiple recipients:

```
dial-peer voice 10 mmoip
 session target marketing-information@mailer.example.com
```

Assuming that mailer.example.com is running sendmail, you can put the following information into its /etc/aliases file:

```
marketing-information:
 john@example.com,
 fax=+14085550112@sj-offramp.example.com
```

The following example configures a session target for VoATM. The session target is sent to ATM interface 0, and is for a PVC with a VPI/VCI of 1/100.

```
dial-peer voice 12 voatm
 destination-pattern 13102221111
 session target atm1/0 pvc 1/100
```

Related Commands

Command	Description
called-number	Enables an incoming VoFR call leg to be bridged to the correct POTS call leg.
codec (dial-peer)	Specifies the voice coder rate of speech for a dial peer.
cptone	Specifies a regional tone, ring, and cadence setting for an analog voice port.
destination-pattern	Specifies either the prefix or full E.164 telephone number (depending on the dial plan) to be used for a dial peer.
dtmf-relay	Enables the DSP to generate FRF.11 Annex A frames for a dial peer.
preference	Indicates the preferred selection order of a dial peer within a hunt group.
session protocol	Establishes a VoFR protocol for calls between local and remote routers via the packet network.
session target	Configures a network-specific address for a dial peer.
session target loopback	Tests the voice transmission path of a call.
signal-type	Sets the signaling type to be used when connecting to a dial peer.

session target (VoFR dial peer)

To specify a network-specific address for a specified VoFR dial peer, use the **session target** command in dial-peer configuration mode. To reset to the default, use the **no** form of this command.

Cisco 2600 Series and Cisco 3600 Series Routers
session target *interface dlci* [*cid*]
no session target

Cisco 7200 Series Routers
session target interface dlci
no session target

Syntax Description

interface	Serial interface and interface number (slot number and port number) associated with this dial peer. For the range of valid interface numbers for the selected interface type, enter a **?** character after the interface type.
dlci	Data link connection identifier for this dial peer. Range is from 16 to 1007.
cid	(Optional) DLCI subchannel to be used for data on FRF.11 calls. A CID must be specified only when the session protocol is **frf11-trunk**. When the session protocol is **cisco-switched**, the CID is dynamically allocated. Range is from 4 to 255. **Note** By default, CID 4 is used for data; CID 5 is used for call-control. We recommend that you select CID values between 6 and 63 for voice traffic. If the CID is greater than 63, the FRF.11 header contains an extra byte of data.

Command Default

The default for this command is enabled with no IP address or domain name defined.

Command Modes

Dial-peer configuration (config-dial-peer)

Command History

Release	Modification
11.3(1)T	This command was introduced.
11.3(1)MA	This command was implemented for VoFR, VoHDLC, and POTS dial peers on the Cisco MC3810.
12.0(3)XG	This command was implemented for VoFR dial peers on the Cisco 2600 series and Cisco 3600 series. The *cid* option was added.
12.0(4)T	This command was integrated into Cisco IOS Release12.0(4)T and implemented for VoFR and POTS dial peers on the Cisco 7200 series.

Usage Guidelines

Use the **session target**command to specify a network-specific address or domain name for a dial peer. Whether you select a network-specific address or a domain name depends on the session protocol you select. The syntax of this command complies with the simple syntax of mailto: as described in RFC 1738.

The **session target loopback** command is used for testing the voice transmission path of a call. The loopback point depends on the call origin and the loopback type selected.

For VoFR dial peers, the *cid* option is not allowed when the **cisco-switched**option for the **session protocol** command is used.

Examples

The following example configures serial interface 1/0, DLCI 100 as the session target for Voice over Frame Relay dial peer 200 (an FRF.11 dial peer) using the FRF.11 session protocol:

```
dial-peer voice 200 vofr
 destination-pattern 13102221111
 called-number 5552150
 session protocol frf11-trunk
 session target serial 1/0 100 20
```

The following example delivers fax-mail to multiple recipients:

```
dial-peer voice 10 mmoip
 session target marketing-information@mailer.example.com
```

Assuming that mailer.example.com is running sendmail, you can put the following information into its /etc/aliases file:

```
marketing-information:
 john@example.com,
 fax=+14085551212@sj-offramp.example.com
```

Related Commands

Command	Description
called-number	Enables an incoming VoFR call leg to be bridged to the correct POTS call leg.
codec (dial-peer)	Specifies the voice coder rate of speech for a dial peer.
cptone	Specifies a regional tone, ring, and cadence setting for an analog voice port.
destination-pattern	Specifies either the prefix or the full E.164 telephone number (depending on the dial plan) to be used for a dial peer.
dtmf-relay	Enables the DSP to generate FRF.11 Annex A frames for a dial peer.
preference	Indicates the preferred selection order of a dial peer within a hunt group.
session protocol	Establishes a VoFR protocol for calls between the local and the remote routers via the packet network.
signal-type	Sets the signaling type to be used when connecting to a dial peer.

session target (VoIP dial peer)

To designate a network-specific address to receive calls from a VoIP or VoIPv6 dial peer, use the **session target** command in dial peer configuration mode. To reset to the default, use the **no** form of this command.

Cisco 1751, Cisco 3725, Cisco 3745, and Cisco AS5300
session target {**dhcp** | **ipv4:***destination-address* | **ipv6:**[*destination-address*] | **dns:**[**s.** | **d.** | **e.** | **u.**] *hostname* | **enum:***table-num* | **loopback:rtp** | **ras** | **sip-server** | **registrar**} [**:***port*]
no session target

Cisco 2600 Series, Cisco 3600 Series, Cisco AS5350, Cisco AS5400, and Cisco AS5850
session target {**dhcp** | **ipv4:***destination-address* | **ipv6:**[*destination-address*] | **dns:**[**s.** | **d.** | **e.** | **u.**] *hostname* | **enum:***table-num* | **loopback:rtp** | **ras** | **settlement** *provider-number* | **sip-server** | **registrar**} [**:***port*]
no session target

Syntax Description

dhcp	Configures the router to obtain the session target via DHCP. **Note** The **dhcp** option can be made available only if the Session Initiation Protocol (SIP) is used as the session protocol. To enable SIP, use the **session protocol** (dial peer) command.
ipv4: *destination -address*	Configures the IP address of the dial peer to receive calls. The colon is required.
ipv6: [*destination-address*]	Configures the IPv6 address of the dial peer to receive calls. Square brackets must be entered around the IPv6 address. The colon is required.
dns:[s] *hostname*	Configures the host device housing the domain name system (DNS) server that resolves the name of the dial peer to receive calls. The colon is required. Use one of the following macros with this keyword when defining the session target for VoIP peers: • **s.** --(Optional) Source destination pattern is used as part of the domain name. • **d.** --(Optional) Destination number is used as part of the domain name. • **e.** --(Optional) Digits in the called number are reversed and periods are added between the digits of the called number. The resulting string is used as part of the domain name. • **u.** --(Optional) Unmatched portion of the destination pattern (such as a defined extension number) is used as part of the domain name. • *hostname* --String that contains the complete hostname to be associated with the target address; for example, serverA.example1.com.
enum: *table -num*	Configures ENUM search table number. Range is from 1 to 15. The colon is required.

loopback:rtp	Configures all voice data to loop back to the source. The colon is required.
ras	Configures the registration, admission, and status (RAS) signaling function protocol. A gatekeeper is consulted to translate the E.164 address into an IP address.
sip -server	Configures the global SIP server is the destination for calls from the dial peer.
: *port*	(Optional) Port number for the dial-peer address. The colon is required.
settlement *provider -number*	Configures the settlement server as the target to resolve the terminating gateway address. • The *provider-number* argument specifies the provider IP address.
registrar	Specifies to route the call to the registrar end point. • The **registrar** keyword is available only for SIP dial peers.

Command Default

No IP address or domain name is defined.

Command Modes

Dial peer configuration (config-dial-peer)

Command History

Release	Modification
11.3(1)T	This command was introduced on the Cisco 2600 series and Cisco 3600 series.
12.0(3)T	This command was modified. This command was implemented on the Cisco AS5300. The **ras** keyword was added.
12.0(4)XJ	This command was implemented for store-and-forward fax on the Cisco AS5300.
12.1(1)T	This command was integrated into Cisco IOS Release 12.1(1)T. The **settlement** and **sip-server** keywords were added.
12.2(2)XA	This command was implemented on the Cisco AS5350 and Cisco AS5400.
12.2(2)XB1	This command was implemented on the Cisco AS5850.
12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T. Support for the Cisco AS5300, Cisco AS5350, Cisco AS5400, and Cisco AS5850 was not included in this release.
12.2(11)T	This command was implemented on the Cisco AS5300, Cisco AS5350, Cisco AS5400, and Cisco AS5850. The **enum** keyword was added.
12.4(22)T	This command was modified. Support for IPv6 was added.
12.4(22)YB	This command was modified. The **dhcp** keyword was added.
15.0(1)M	This command was integrated into Cisco IOS Release 15.0(1)M.

Release	Modification
Cisco IOS XE Amsterdam 17.2.1r	Introduced support for YANG models.

Usage Guidelines

Use the **session target** command to specify a network-specific destination for a dial peer to receive calls from the current dial peer. You can select an option to define a network-specific address or domain name as a target, or you can select one of several methods to automatically determine the destination for calls from the current dial peer.

Use the **session target dns** command with or without the specified macros. Using the optional macros can reduce the number of VoIP dial-peer session targets that you must configure if you have groups of numbers associated with a particular router.

The **session target enum** command instructs the dial peer to use a table of translation rules to convert the dialed number identification service (DNIS) number into a number in E.164 format. This translated number is sent to a DNS server that contains a collection of URLs. These URLs identify each user as a destination for a call and may represent various access services, such as SIP, H.323, telephone, fax, e-mail, instant messaging, and personal web pages. Before assigning the session target to the dial peer, configure an ENUM match table with the translation rules using the **voice enum-match-table**command in global configuration mode. The table is identified in the **session target enum** command with the *table-num* argument.

Use the **session target loopback** command to test the voice transmission path of a call. The loopback point depends on the call origin.

Use the **session target dhcp** command to specify that the session target host is obtained via DHCP. The **dhcp** option can be made available only if the SIP is being used as the session protocol. To enable SIP, use the **session protocol**(dial peer) command.

In Cisco IOS Release 12.1(1)T the **session target** command configuration cannot combine the target of RAS with the **settle-call** command.

For the **session target settlement** *provider-number* command, when the VoIP dial peers are configured for a settlement server, the *provider-number* argument in the **session target** and **settle-call** commands should be identical.

Use the **session target sip-server** command to name the global SIP server interface as the destination for calls from the dial peer. You must first define the SIP server interface by using the **sip-server** command in SIP user-agent (UA) configuration mode. Then you can enter the **session target sip-server** option for each dial peer instead of having to enter the entire IP address for the SIP server interface under each dial peer.

After the SIP endpoints are registered with the SIP registrar in the hosted unified communications (UC), you can use the **session target registrar** command to route the call automatically to the registrar end point. You must configure the **session target** command on a dial pointing towards the end point.

Examples

The following example shows how to create a session target using DNS for a host named "voicerouter" in the domain example.com:

```
dial-peer voice 10 voip
 session target dns:voicerouter.example.com
```

The following example shows how to create a session target using DNS with the optional **u**. macro. In this example, the destination pattern ends with four periods (.) to allow for any four-digit extension that has the leading number 1310555. The optional **u**. macro directs the gateway to use the

unmatched portion of the dialed number--in this case, the four-digit extension--to identify a dial peer. The domain is "example.com."

```
dial-peer voice 10 voip
 destination-pattern 1310555....
 session target dns:$u$.example.com
```

The following example shows how to create a session target using DNS, with the optional **d**. macro. In this example, the destination pattern has been configured to 13105551111. The optional macro **d**. directs the gateway to use the destination pattern to identify a dial peer in the "example.com" domain.

```
dial-peer voice 10 voip
 destination-pattern 13105551111
 session target dns:$d$.example.com
```

The following example shows how to create a session target using DNS, with the optional **e**. macro. In this example, the destination pattern has been configured to 12345. The optional macro **e**. directs the gateway to do the following: reverse the digits in the destination pattern, add periods between the digits, and use this reverse-exploded destination pattern to identify the dial peer in the "example.com" domain.

```
dial-peer voice 10 voip
 destination-pattern 12345
 session target dns:$e$.example.com
```

The following example shows how to create a session target using an ENUM match table. It indicates that calls made using dial peer 101 should use the preferential order of rules in enum match table 3:

```
dial-peer voice 101 voip
 session target enum:3
```

The following example shows how to create a session target using DHCP:

```
dial-peer voice 1 voip
session protocol sipv2
voice-class sip outbound-proxy dhcp
session target dhcp
```

The following example shows how to create a session target using RAS:

```
dial-peer voice 11 voip
 destination-pattern 13105551111
 session target ras
```

The following example shows how to create a session target using settlement:

```
dial-peer voice 24 voip
 session target settlement:0
```

The following example shows how to create a session target using IPv6 for a host at 2001:10:10:10:10:10:10:230a:5090:

```
dial-peer voice 4 voip
destination-pattern 5000110011
session protocol sipv2
```

```
session target ipv6:[2001:0DB8:10:10:10:10:10:230a]:5090
codec g711ulaw
```

The following example shows how to configure Cisco Unified Border Element (UBE) to route a call to the registering end point:

```
dial-peer voice 4 voip
session target registrar
```

Related Commands

Command	Description
destination-pattern	Specifies either the prefix or the full E.164 telephone number (depending on the dial plan) to be used for a dial peer.
dial -peer voice	Enters dial peer configuration mode and specifies the method of voice-related encapsulation.
session protocol (dial peer)	Specifies a session protocol for calls between local and remote routers using the packet network dial peer configuration mode.
settle -call	Specifies that settlement is to be used for the specified dial peer, regardless of the session target type.
sip -server	Defines a network address for the SIP server interface.
voice enum -match-table	Initiates the ENUM match table definition.

session target

To configure the Session Initiation Protocol (SIP) Uniform Resource Locator (URI) as the session target for a dial peer, use the **session target sip-uri** command in dial peer voice configuration mode. To disable this configuration, use the **no** form of the command.

session target
no session target

Command Default

Command Modes

Dial peer voice configuration (config-dial-peer)

Command History

Release	Modification
15.4(1)T	This command was introduced.

Usage Guidelines

Example

The following example shows how to configure the SIP URI as the session target for a dial peer using the **session target sip-uri** command:

```
Device> enable
Device# configure terminal
Device(config)# dial-peer voice 25 voip
Device(config-dial-peer)# session protocol sipv2
Device(config-dial-peer)# destination uri mydesturi
Device(config-dial-peer)# session target sip-uri
Device(config-dial-peer)# end
```

session transport

To configure a VoIP dial peer to use TCP or User Datagram Protocol (UDP) as the underlying transport layer protocol for Session Initiation Protocol (SIP) messages, use the **session transport** command in dial-peer configuration mode. To reset to the **system** default keyword, use the **no** form of this command.

session transport {**system** | **tcp** [**tls**] | **udp**}
no session transport {**system** | **tcp** [**tls**] | **udp**}

Syntax Description

system	The SIP dial peer defers to the voice service VoIP session transport.
tcp	The SIP dial peer uses the TCP transport layer protocol.
tls	(Optional) The SIP dial peer uses Transport Layer Security (TLS) over the TCP transport layer protocol.
udp	The SIP dial peer uses the UDP transport layer protocol. This is the default.

Command Default

UDP

Note The transport protocol specified with the **transport**command **must match**the one specified with this command.

Command Modes

Dial-peer configuration.

Voice class tenant.

Command History

Release	Modification
12.1(1)T	This command was introduced on the Cisco 2600 series, Cisco 3600 series, and Cisco AS5300.
12.2(2)XA	This command was implemented on the Cisco AS5350 and Cisco AS5400.
12.2(2)XB1	This command was implemented on the Cisco AS5850.
12.2(11)T	This command was integrated into Cisco IOS Release 12.2(11)T.
12.4(6)T	The optional tls keyword was added to the command.
Cisco IOS XE Cupertino 17.7.1a	Introduced support for YANG models.

Usage Guidelines

Use the show **sip-ua** status command to ensure that the transport protocol that you set using this command matches the protocol set using the **transport** command. The **transport** command is used in dial-peer configuration mode to specify the SIP transport method, either UDP, TCP, or TLS over TCP.

Examples

The following example shows a VoIP dial peer configured to use TCP as the underlying transport layer protocol for SIP messages:

```
dial-peer voice 102 voip
 session transport tcp
```

The following example shows a VoIP dial peer configured to use TLS over TCP as the underlying transport layer protocol for SIP messages:

```
dial-peer voice 102 voip
 session transport tcp tls
```

The following example shows a VoIP dial peer configured to use UDP as the underlying transport layer protocol for SIP messages:

```
dial-peer voice 102 voip
 session transport udp
```

Related Commands

Command	Description
show sip-ua status	Displays the status of SIP call service on a SIP gateway.
transport	Configures the SIP user agent (gateway) for SIP signaling messages on inbound calls through the SIP TCP or UDP socket.

session transport (H.323 voice-service)

To configure the underlying transport layer protocol for H.323 messages to be used across all VoIP dial peers, use the **session transport** command in H.323 voice service configuration mode. To reset the default value, use the **no** form of this command.

session transport {**udp** | **tcp** [**calls-per-connection** *value*]}
no session transport

Syntax Description

udp	Configures the H.323 dial peer to use the UDP transport layer protocol.
tcp	Configures the H.323 dial peer to use the TCP transport layer protocol. This is the default.
calls-per-connection	Configures the number of calls multiplexed into a single TCP connection.
value	The number of calls. The range is from 1 to 9999. The default is 5.

Command Default

TCP is the default session transport protocol; the default **calls-per-connection** value is 5.

Command Modes

H.323 voice-service configuration (conf-serv-h323)

Command History

Release	Modification
12.2(1)T	This command was introduced for session initiation protocol (SIP) dial peers.
12.2(2)XA	This command was modified to include support for H323 dial peers and to include the **calls-per-connection** keyword.
12.2(4)T	This command was integrated into Cisco IOS Release 12.2(4)T.
12.2(2)XB1	This command was implemented on the Cisco AS5850.
12.2(11)T	This command was integrated into Cisco IOS Release 12.2(11)T.

Examples

The following example shows a dial peer configured to use the UDP transport layer protocol.

```
Router(conf-voi-serv)# h323
Router(conf-serv-h323)# session transport udp
```

Related Commands

Command	Description
h323	Enables H.323 voice service configuration commands.

session transport (SIP)

To configure the underlying transport layer protocol for SIP messages to TCP, transport layer security over TCP (TLS over TCP), or User Datagram Protocol (UDP), use the session transport command in SIP configuration mode. To reset the value of this command to the default, use the **no** form of this command.

session transport {**udp** | **tcp** [**tls**]}
no session transport {**udp** | **tcp** [**tls**]}

Syntax Description

udp	Configure SIP messages to use the UDP transport layer protocol. This is the default.
tcp	Configure SIP messages to use the TCP transport layer protocol.
tls	(Optional) Configure SIP messages to use the TLS over TCP transport layer protocol.

Command Default

The default for the command is UDP.

Command Modes

Voice service SIP configuration (conf-serv-sip)

Command History

Release	Modification
12.2(2)XB	This command was introduced in SIP configuration mode.
12.2(2)XB2	This command was implemented on the Cisco AS5850 platform.
12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T and support was added for the Cisco 3700 series. Cisco AS5300, Cisco AS5350, Cisco AS5850, and Cisco AS5400 platforms were not supported in this release.
12.2(11)T	Support was added for the Cisco AS5300, Cisco AS5350, Cisco AS5400, and Cisco AS5850 platforms.
12.4(6)T	The optional tls keyword was added to the command.
Cisco IOS XE Amsterdam 17.2.1r	Introduced support for YANG models.

Usage Guidelines

Use the **show sip-ua status** command to verify that the transport protocol set with the **session transport**command matches the protocol set using the **transport** command in SIP user agent configuration mode.

Examples

The following example configures the underlying transport layer protocol for SIP messages to UDP:

```
voice service voip
 sip
 session transport udp
```

The following example configures the underlying transport layer protocol for SIP messages to TCP:

```
voice service voip
 sip
 session transport tcp
```

The following example configures the underlying transport layer protocol for SIP messages to TLS over TCP:

```
voice service voip
 sip
 session transport tcp tls
```

Related Commands

Command	Description
show sip-ua status	Displays the status of SIP call service on a SIP gateway.
transport	Configures the SIP gateway for SIP signaling messages on inbound calls through the SIP TCP or UDP socket.

session-set

To create a Signlaing System 7 (SS7)-link-to-SS7-session-set association or to associate an SS7 link with an SS7 session set on the Cisco 2600-based Signaling Link Terminal (SLT), enter the session-set command in global configuration mode. To remove the link from its current SS7 session set and to add it to SS7 session set 0 (the default), use the no form of this command.

session-set *session-set-id*
no session-set

Syntax Description

session -set-id	SS7 session ID. Valid values are 0 and 1. Default is 0.

Command Default

SS7 session set 0

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(15)T	This command was introduced on the Cisco 2600-based SLT.

Usage Guidelines

On Cisco AS5350 and Cisco AS5400 platforms, the **channel-id** command is used to create an SS7-link-to-SS7-session-set association on the Cisco SLT. The Cisco 26xx platforms do not support the **channel-id** command, so channel IDs on the Cisco 26xx-based SLT are implicitly assigned on the basis of the slot location of the WAN interface card (WIC) and the channel group ID used to create the SS7 link.

If this command is omitted, the link is implicitly added to the SS7 session set 0, which is the default.

Examples

The following example shows how the **session-set** command is used to add the associated SS7 link to an SS7 session set:

```
session-set 1
```

The following example shows how the no session-set command is used to remove the link from its current SS7 session set and add it to SS7 session set 0, which is the default:

```
no session-set
```

Related Commands

Command	Description
channel-id	Assigns a session channel ID to a Signaling System 7 (SS7) serial link or assign an SS7 link to an SS7 session set on a Cisco AS5350 or Cisco AS5400.

session-timeout

To specify the maximum amount of time for which a TFTP session can remain open, use the **session-timeout** command in phone proxy configuration mode. To remove the timeout period of a TFTP session, use the **no** form of the command.

session-timeout *seconds*
no session-timeout

Syntax Description

seconds	Maximum length of a TFTP session in seconds. The range is from 60 to 6000. The default is 180 seconds.

Command Default

The session timeout is 180 seconds.

Command Modes

Phone proxy configuration mode (config-phone-proxy)

Command History

Release	Modification
15.3(3)M	This command was introduced.

Usage Guidelines

Example

The following example shows how to specify a timeout period for a TFTP session of 200 seconds:

```
Device(config)# voice-phone-proxy first-pp
Device(config-phone-proxy)# session-timeout 200
```

set

To create a fault-tolerant or nonfault-tolerant session set with the client or server option, use the **set** command in backhaul session-manager configuration mode. To delete the set, use the **no** form of this command.

set *set-name* {**client** | **server**} {**ft** | **nft**}
no set *set-name* {**client** | **server**} {**ft** | **nft**}

Syntax Description

set-name	Session-set name.
client	The session set operates as a client. Select this option for signaling backhaul.
server	The session set operates as a server.
ft	Fault-tolerant operation. Select fault-tolerant if this session set can contain more than one session group, with each session group connecting the gateway to a different Cisco VSC3000. Fault-tolerance allows the system to operate properly if a session group in the session set fails.
nft	Non-fault-tolerant operation. Select non-fault-tolerant if this session set contains only one session group (which connects the gateway to a single Cisco VSC3000).

Command Default

No default behavior or values

Command Modes

Backhaul session manager configuration (config-bsm)

Command History

Release	Modification
12.1(1)T	This command was introduced.
12.2(4)T	This command was implemented on the Cisco 2600 series, Cisco 3600 series, and Cisco MC3810.
12.2(2)XB	This command was implemented on the Cisco AS5350 and Cisco AS5400.
12.2(2)XB1	This command was implemented on the Cisco AS5850.
12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T and was implemented on the Cisco IAD2420 series. Support for on the Cisco AS5350, Cisco AS5400, and Cisco AS5850 is not included in this release.
12.2(11)T	This command is supported on the Cisco AS5350, Cisco AS5400, and Cisco AS5850 in this release.

Usage Guidelines

Multiple session groups can be associated with a session set.

For signaling backhaul, session sets should be configured to operate as clients.

A session set cannot be deleted unless all session groups associated with the session set are deleted first.

Examples

The following example sets the client set named "set1" as fault-tolerant:

```
Router(config-bsm)# set set1 client ft
```

set http client cache stale

To set the status of all entries in the HTTP client cache to stale, use the **set http client cache stale** command in global configuration mode.

set http client cache stale

Syntax Description

This command has no arguments or keywords.

Command Default

Entries in the HTTP client cache are not marked stale manually.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.4(15)T	This command was introduced.
12.4(20)T	This command was integrated into Cisco IOS Release 12.4(20)T.

Usage Guidelines

Use this command to force the HTTP client to check with the server to see if an updated version of the file exists when any cached entries are requested by the VoiceXML application. If the router is in nonstreaming mode, a conditional reload is sent to the HTTP server. If the router is in streaming mode, an unconditional reload is sent for the refresh. Regardless of which mode the router is in, the VoiceXML application is guaranteed to receive the most up-to-date file when you use the **set http client cache stale** command.

The **show http client cache** command shows a pound sign (#) next to the age of entries that are marked stale manually.

Examples

The following example sets the status of all entries in the HTTP client cache to stale:

```
Router# set http client cache stale
```

Related Commands

Command	Description
show http client cache	Displays information about the entries contained in the HTTP client cache.

set pstn-cause

To map an incoming PSTN cause code to a Session Initiation Protocol (SIP) error status code, use the **set pstn-cause**command in SIP user-agent configuration mode. To reset to the default, use the **no** form of this command.

set pstn-cause *value* **sip-status** *value*
no set pstn-cause

Syntax Description

pstn -cause *value*	PSTN cause code. Range is from 1 to 127
sip -status *value*	SIP status code that is to correspond with the PSTN cause code. Range is from 400 to 699.

Command Default

The default mappings defined in the following table are used:

Table 5: Default PSTN Cause Codes Mapped to SIP Events

PSTN Cause Code	Description	SIP Event
1	Unallocated number	404 Not found
2	No route to specified transit network	404 Not found
3	No route to destination	404 Not found
17	User busy	486 Busy here
18	No user responding	480 Temporarily unavailable
19	No answer from the user	
20	Subscriber absent	
21	Call rejected	403 Forbidden
22	Number changed	410 Gone
26	Non-selected user clearing	404 Not found
27	Destination out of order	404 Not found
28	Address incomplete	484 Address incomplete
29	Facility rejected	501 Not implemented
31	Normal, unspecified	404 Not found
34	No circuit available	503 Service unavailable
38	Network out of order	503 Service unavailable
41	Temporary failure	503 Service unavailable

PSTN Cause Code	Description	SIP Event
42	Switching equipment congestion	503 Service unavailable
47	Resource unavailable	503 Service unavailable
55	Incoming class barred within the Closed User Group (CUG)	403 Forbidden
57	Bearer capability not authorized	403 Forbidden
58	Bearer capability not currently available	501 Not implemented
65	Bearer capability not implemented	501 Not implemented
79	Service or option not implemented	501 Not implemented
87	User not member of the Closed User Group (CUG)	503 Service unavailable
88	Incompatible destination	400 Bad request
95	Invalid message	400 Bad request
102	Recover on Expires timeout	408 Request timeout
111	Protocol error	400 Bad request
Any code other than those listed above	500 Internal server error	

Command Modes

SIP UA configuration (config-sip-ua)

Command History

Release	Modification
12.2(2)XB	This command was introduced.
12.2(2)XB2	This command was implemented on the Cisco AS5850.
12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T. Support for on the Cisco AS5300 Cisco AS5350, Cisco AS5400, and Cisco AS5850 is not included in this release.
Cisco IOS XE Cupertino 17.7.1a	Introduced support for YANG models.

Usage Guidelines

A PSTN cause code can be mapped only to one SIP status code at a time.

Examples

The following example maps a SIP status code to correspond to a PSTN cause code:

```
Router(config)# sip-ua
Router(config-sip-ua)# set pstn-cause 111 sip-status 400
Router(config-sip-ua)# exit
```

Related Commands

Command	Description
set sip -status	Sets an incoming SIP error status code to a PSTN release cause code.

set sip-status

To map an incoming Session Initiation Protocol (SIP) error status code to a PSTN cause code, use the **set sip-status**command in SIP user-agent configuration mode. To reset to the default, use the **no** form of this command.

set sip-status *value* **pstn-cause** *value*
no set sip-status

Syntax Description

sip -status *value*	SIP status code. Range is from 400 to 699.
pstn -cause *value*	PSTN cause code that is to correspond with the SIP status code. Range is from 1 to 127.

Command Default

The default mappings defined in the table below are used:

Table 6: Default SIP Events Mapped to PSTN Cause Codes

SIP Event	PSTN Cause Code	Description
400 Bad request	127	Interworking, unspecified
401 Unauthorized	57	Bearer capability not authorized
402 Payment required	21	Call rejected
403 Forbidden	57	Bearer capability not authorized
404 Not found	1	Unallocated number
405 Method not allowed	127	Interworking, unspecified
406 Not acceptable		
407 Proxy authentication required	21	Call rejected
408 Request timeout	102	Recover on Expires timeout
409 Conflict	41	Temporary failure
410 Gone	1	Unallocated number
411 Length required	127	Interworking, unspecified
413 Request entity too long		
414 Request URI (URL) too long		
415 Unsupported media type	79	Service or option not available
420 Bad extension	127	Interworking, unspecified
480 Temporarily unavailable	18	No user response

SIP Event	PSTN Cause Code	Description
481 Call leg does not exist	127	Interworking, unspecified
482 Loop detected		
483 Too many hops		
484 Address incomplete	28	Address incomplete
485 Address ambiguous	1	Unallocated number
486 Busy here	17	User busy
487 Request canceled	127	Interworking, unspecified
488 Not acceptable here	127	Interworking, unspecified
500 Internal server error	41	Temporary failure
501 Not implemented	79	Service or option not implemented
502 Bad gateway	38	Network out of order
503 Service unavailable	63	Service or option unavailable
504 Gateway timeout	102	Recover on Expires timeout
505 Version not implemented	127	Interworking, unspecified
580 Precondition failed	47	Resource unavailable, unspecified
600 Busy everywhere	17	User busy
603 Decline	21	Call rejected
604 Does not exist anywhere	1	Unallocated number
606 Not acceptable	58	Bearer capability not currently available

Command Modes

SIP UA configuration (config-sip-ua)

Command History

Release	Modification
12.2(2)XB	This command was introduced.
12.2(2)XB2	This command was implemented on the Cisco AS5850.
12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T. Support for the Cisco AS5300, Cisco AS5350, Cisco AS5400, and Cisco AS5850 is not included in this release.
Cisco IOS XE Cupertino 17.7.1a	Introduced support for YANG models.

Usage Guidelines

A SIP status code can be mapped to many PSTN cause codes. For example, 503 can be mapped to 34, 38, and 58.

Examples

The following example maps a PSTN cause code to correspond to a SIP status code:

```
Router(config)# sip-ua
Router(config-sip-ua)# set sip-status 400 pstn-cause 16
```

Related Commands

Command	Description
set pstn -cause	Sets an incoming PSTN cause code to a SIP error status code.

settle-call

To force a call to be authorized with a settlement server that uses the address resolution method specified in the **session target** command, use the **settle-call**command in dial-peer configuration mode. To ensure that no authorization is performed by a settlement server, use the **no** form of this command.

settle-call *provider-number*
no settle-call *provider-number*

Syntax Description

provider -number	Digit defining the ID of a particular settlement server. The only valid entry is 0. **Note** If **session target** *type* is **settlement**, the *provider-number* argument in the **session target** and **settle-call** commands should be identical.

Command Default

No default behavior or values.

Command Modes

Dial-peer configuration (config-dial-peer)

Command History

Release	Modification
12.1(1)T	This command was introduced on the Cisco 2600 series, Cisco 3600 series, and Cisco AS5300.

Usage Guidelines

With the **session target** command, a dial peer can determine the address of the terminating gateway through the **ipv4**, **dns**, **ras,** and **settlement** keywords.

If the session target is not **settlement,** and the **settle-call** *provider-number* argument is set, the gateway resolves address of the terminating gateway using the specified method and then requests the settlement server to authorize that address and create a settlement token for that particular address. If the server cannot authorize the terminating gateway address suggested by the gateway, the call fails.

Do not combine the session target types **ras** and **settle-call**. Combination of session target types is not supported.

Examples

The following example sets a call to be authorized with a settlement server that uses the address resolution method specified in the **session target**:

```
dial-peer voice 10 voip
 destination-pattern 1408.......
 session target ipv4:172.22.95.14
 settle-call 0
```

Related Commands

Command	Description
session target	Specifies a network-specific address for a specified dial peer.

settlement

To enter settlement configuration mode and specify the attributes specific to a settlement provider, use the **settlement** command in global configuration mode. To disable the settlement provider, use the **no** form of this command.

settlement *provider-number*
no settlement *provider-number*

Syntax Description

provider -number	Digit that defines a particular settlement server. The only valid entry is 0.

Command Default

0

Command Modes

Global configuration (config)

Command History

Release	Modification
12.0(4)XH1	This command was introduced on the Cisco 2600 series, Cisco 3600 series, and Cisco AS5300.
12.1(1)T	This command was integrated into Cisco IOS Release 12.1(1)T.

Usage Guidelines

The variable *provider-number* defines a particular settlement provider. For Cisco IOS Release 12.1, only one clearinghouse per system is allowed, and the only valid value for *provider-number* is 0.

Examples

This example enters settlement configuration mode:

```
settlement 0
```

Related Commands

Command	Description
connection -timeout	Configures the length of time for which a connection is maintained after a communication exchange is completed.
customer -id	Identifies a carrier or ISP with a settlement provider.
device -id	Specifies a gateway associated with a settlement provider.
encryption	Sets the encryption method to be negotiated with the provider.
max -connection	Sets the maximum number of simultaneous connections to be used for communication with a settlement provider.
response -timeout	Configures the maximum time to wait for a response from a server.
retry -delay	Sets the time between attempts to connect with the settlement provider.
retry -limit	Sets the connection retry limit.

Command	Description
session -timeout	Sets the interval for closing the connection when there is no input or output traffic.
show settlement	Displays the configuration for all settlement server transactions.
shutdown	Brings up the settlement provider.
type	Configures an SAA-RTR operation type.

settlement roam-pattern

To configure a pattern that must be matched to determine if a user is roaming, use the **settlement roam-pattern**command in global configuration mode. To delete a particular pattern, use the **no** form of this command.

settlement *provider-number* **roam-pattern** *pattern* {**roaming** | **noroaming**}
no settlement *provider-number* **roam-pattern** *pattern* {**roaming** | **noroaming**}

Syntax Description

provider -number	Digit defining the ID of particular settlement server. The only valid entry is 0.
pattern	User account pattern.
roaming	Specifies that a user is roaming.
noroaming	Specifies that a user is not roaming.

Command Default

No default pattern is configured.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.1(1)T	This command was introduced on the Cisco 2600 series, Cisco 3600 series, and Cisco AS5300.

Usage Guidelines

Multiple roam patterns can be entered on one gateway.

Examples

The following example shows how to configure a pattern that determines if a user is roaming:

```
settlement 0 roam-pattern 1222 roaming
settlement 0 roam-pattern 1333 noroaming
settlement 0 roam-pattern 1444 roaming
settlement 0 roam-pattern 1555 noroaming
```

Related Commands

Command	Description
roaming (settlement)	Enables the roaming capability for a settlement provider.
settlement	Enters settlement configuration mode.

sgcp

To start and allocate resources for the Simple Gateway Control Protocol (SGCP) daemon, use the **sgcp** command in global configuration mode. To terminate all calls, release all allocated resources, and kill the SGCP daemon, use the **no** form of this command.

sgcp
no sgcp

Syntax Description

This command has no arguments or keywords.

Command Default

The SGCP daemon is not enabled.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.0(5)T	This command was introduced in a private release on the Cisco AS5300 only and was not generally available.
12.0(7)XK	This command was implemented on the Cisco MC3810 and the Cisco 3600 series (except for the Cisco 3620) in a private release that was not generally available.
12.1(2)T	This command was implemented on the Cisco 3600 series and Cisco MC3810.

Usage Guidelines

When the SGCP daemon is not active, all SGCP messages are ignored.

When you enter the **no sgcp** command, the SGCP process is removed.

Note After you enter the **no sgcp** command, you must save the configuration and reboot the router for the disabling of SGCP to take effect.

Examples

The following example enables the SGCP daemon:

```
sgcp
```

The following example disables the SGCP daemon:

```
no sgcp
```

Related Commands

Command	Description
sgcp call-agent	Defines the IP address of the default SGCP call agent.
sgcp graceful-shutdown	Gracefully terminates all SGCP activity.

Command	Description
sgcp max-waiting-delay	Sets the SGCP maximum waiting delay to prevent restart avalanches.
sgcp modem passthru	Enables SGCP modem or fax pass-through.
sgcp quarantine-buffer disable	Disables the SGCP quarantine buffer.
sgcp request retries	Specifies the number of times to retry sending "notify" and "delete" messages to the SGCP call agent.
sgcp request timeout	Specifies how long the system should wait for a response to a request.
sgcp restart	Triggers the router to send an RSIP message to the SGCP call agent indicating that the T1 controller is up or down so that the call agent can synchronize with the T1 controller.
sgcp retransmit timer	Configures the SGCP retransmission timer to use a random algorithm method.
sgcp timer	Configures how the gateway detects the RTP stream host.
sgcp tse payload	Enables Inband TSE for fax/modem operation.

sgcp call-agent

To define the IP address of the default Simple Gateway Control Protocol (SGCP) call agent in the router configuration file, use the **sgcp call-agent** command in global configuration mode. To remove the IP address of the default SGCP call agent from the router configuration, use the **no** form of this command.

sgcp call-agent *ipaddress* [**:** *udp port*]
no sgcp call-agent *ipaddress*

Syntax Description

ipaddress	IP address or hostname of the call agent.
:udp port	(Optional) UDP port of the call agent.

Command Default

No IP address is configured.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.0(5)T	This command was introduced in a private release on the Cisco AS5300 only and was not generally available.
12.0(7)XK	This command was implemented on the Cisco MC3810 and the Cisco 3600 series (except for the Cisco 3620) in a private release that was not generally available.
12.1(2)T	This command was implemented on the Cisco 3600 series and Cisco MC3810.

Usage Guidelines

This command defines the IP address of the default SGCP call agent to which the router sends an initial RSIP (Restart In Progress) packet when the router boots up. This is used for initial bootup only before the SGCP call agent contacts the router acting as the gateway.

When you enter the **no sgcp call-agent** command, only the IP address of the default SGCP call agent is removed.

Examples

The following example enables SGCP and specifies the IP address of the call agent:

```
sgcp
sgcp call-agent 209.165.200.225
```

Related Commands

Command	Description
sgcp	Starts and allocates resources for the SGCP daemon.
sgcp graceful-shutdown	Gracefully terminates all SGCP activity.
sgcp max-waiting-delay	Sets the SGCP maximum waiting delay to prevent restart avalanches.
sgcp modem passthru	Enables SGCP modem or fax pass-through.

Command	Description
sgcp quarantine-buffer disable	Disables the SGCP quarantine buffer.
sgcp request retries	Specifies the number of times to retry sending "notify" and "delete" messages to the SGCP call agent.
sgcp request timeout	Specifies how long the system should wait for a response to a request.
sgcp restart	Triggers the router to send an RSIP message to the SGCP call agent indicating that the T1 controller is up or down so that the call agent can synchronize with the T1 controller.
sgcp retransmit timer	Configures the SGCP retransmission timer to use a random algorithm method.
sgcp timer	Configures how the gateway detects the RTP stream host.
sgcp tse payload	Enables Inband TSE for fax/modem operation.

sgcp graceful-shutdown

To block all new calls and gracefully terminate all existing calls (wait for the caller to end the call), use the **sgcp graceful-shutdown**command in global configuration mode. To unblock all calls and allow new calls to go through, use the **no** form of this command.

sgcp graceful-shutdown
no sgcp graceful-shutdown

Syntax Description

This command has no arguments or keywords.

Command Default

No default behavior or values.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.0(5)T	This command was introduced in a private release on the Cisco AS5300 and was not generally available.
12.0(7)XK	This command was implemented on the Cisco MC3810 and Cisco 3600 series (except for the Cisco 3620) in a private release that was not generally available.
12.1(2)T	This command was implemented on the Cisco 3600 series and Cisco MC3810.

Usage Guidelines

Once you issue this command, all requests for new connections (CreateConnection requests) are denied. All existing calls are maintained until users terminate them, or until you enter the **no sgcp**command. When the last active call is terminated, the SGCP daemon is terminated, and all resources allocated to it are released.

Examples

The following example blocks all new calls and terminates existing calls:

```
sgcp graceful-shutdown
```

Related Commands

Command	Description
sgcp	Starts and allocates resources for the SGCP daemon.
sgcp call-agent	Defines the IP address of the default SGCP call agent.
sgcp max-waiting-delay	Sets the SGCP maximum waiting delay to prevent restart avalanches.
sgcp modem passthru	Enables SGCP modem or fax pass-through.
sgcp quarantine-buffer disable	Disables the SGCP quarantine buffer.
sgcp request retries	Specifies the number of times to retry sending "notify" and "delete" messages to the SGCP call agent.

Command	Description
sgcp request timeout	Specifies how long the system should wait for a response to a request.
sgcp restart	Triggers the router to send an RSIP message to the SGCP call agent indicating that the T1 controller is up or down so that the call agent can synchronize with the T1 controller.
sgcp retransmit timer	Configures the SGCP retransmission timer to use a random algorithm method.
sgcp timer	Configures how the gateway detects the RTP stream host.
sgcp tse payload	Enables Inband TSE for fax/modem operation.

sgcp max-waiting-delay

To set the Simple Gateway Control Protocol (SGCP) maximum waiting delay to prevent restart avalanches, use the **sgcp max-waiting-delay**command in global configuration mode. To reset to the default, use the **no** form of this command.

sgcp max-waiting-delay *delay*
no sgcp max-waiting-delay *delay*

Syntax Description

delay	Maximum waiting delay (MWD), in milliseconds. Range is from 0 to 600000. Default is 3000.

Command Default

3,000 ms

Command Modes

Global configuration (config)

Command History

Release	Modification
12.0(5)T	This command was introduced in a private release on the Cisco AS5300, and was not generally available.
12.0(7)XK	This command was implemented on the Cisco MC3810 and the Cisco 3600 series (except for the Cisco 3620) in a private release that was not generally available.
12.1(2)T	This command was implemented on the Cisco 3600 series and the Cisco MC3810.

Examples

The following example sets the maximum wait delay value to 40 ms:

```
sgcp max-waiting-delay 40
```

Related Commands

Command	Description
sgcp	Starts and allocates resources for the SGCP daemon.
sgcp call-agent	Defines the IP address of the default SGCP call agent.
sgcp graceful-shutdown	Gracefully terminates all SGCP activity.
sgcp modem passthru	Enables SGCP modem or fax pass-through.
sgcp quarantine-buffer disable	Disables the SGCP quarantine buffer.
sgcp request retries	Specifies the number of times to retry sending "notify" and "delete" messages to the SGCP call agent.
sgcp request timeout	Specifies how long the system should wait for a response to a request.

Command	Description
sgcp restart	Triggers the router to send an RSIP message to the SGCP call agent indicating that the T1 controller is up or down so that the call agent can synchronize with the T1 controller.
sgcp retransmit timer	Configures the SGCP retransmission timer to use a random algorithm method.
sgcp timer	Configures how the gateway detects the RTP stream host.
sgcp tse payload	Enables Inband TSE for fax/modem operation.

sgcp modem passthru

To enable Simple Gateway Control Protocol (SGCP) modem or fax pass-through, use the **sgcp modem passthru** command in global configuration mode. To disable SGCP modem or fax pass-through, use the **no** form of this command.

sgcp modem passthru {**ca** | **cisco** | **nse**}
no sgcp modem passthru {**ca** | **cisco** | **nse**}

Syntax Description

ca	Call-agent-controlled modem upspeed-method violation message.
cisco	Cisco-proprietary upspeed method based on the protocol.
nse	NSE-based modem upspeed method.

Command Default

SGCP modem or fax pass-through is disabled by default.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.0(7)XK	This command was introduced on the Cisco MC3810 and the Cisco 3600 series (except the Cisco 3620) in a private release that was not generally available.
12.1(2)T	This command was implemented on the Cisco 3600 series and the Cisco MC3810.

Usage Guidelines

You can use this command for fax pass-through because the answer tone can come from either modem or fax transmissions. The upspeed method is the method used to dynamically change the codec type and speed to meet network conditions.

If you use the **nse** option, you must also configure the **sgcp tse payload** command.

Examples

The following example configures SGCP modem pass-through using the call-agent upspeed method:

```
sgcp modem passthru ca
```

The following example configures SGCP modem pass-through using the proprietary Cisco upspeed method:

```
sgcp modem passthru cisco
```

The following example configures SGCP modem pass-through using the NSE-based modem upspeed:

```
sgcp modem passthru nse
sgcp tse payload 110
```

Related Commands

Command	Description
sgcp	Starts and allocates resources for the SGCP daemon.
sgcp call-agent	Defines the IP address of the default SGCP call agent.
sgcp graceful-shutdown	Gracefully terminates all SGCP activity.
sgcp max-waiting-delay	Sets the SGCP maximum waiting delay to prevent restart avalanches.
sgcp quarantine-buffer disable	Disables the SGCP quarantine buffer.
sgcp request retries	Specifies the number of times to retry sending "notify" and "delete" messages to the SGCP call agent.
sgcp request timeout	Specifies how long the system should wait for a response to a request.
sgcp restart	Triggers the router to send an RSIP message to the SGCP call agent indicating that the T1 controller is up or down so that the call agent can synchronize with the T1 controller.
sgcp retransmit timer	Configures the SGCP retransmission timer to use a random algorithm method.
sgcp timer	Configures how the gateway detects the RTP stream host.
sgcp tse payload	Enables Inband TSE for fax/modem operation.

sgcp quarantine-buffer disable

To disable the Simple Gateway Control Protocol (SGCP) quarantine buffer, use the **sgcp quarantine-buffer disable**command in global configuration mode. To reenable the SGCP quarantine buffer, use the **no** form of this command.

sgcp quarantine-buffer disable
no sgcp quarantine-buffer disable

Syntax Description

This command has no arguments or keywords.

Command Default

The SGCP quarantine buffer is enabled.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.0(7)XK	This command was introduced on the Cisco MC3810 and the Cisco 3600 series (except for the Cisco 3620) in a private release that was not generally available.
12.1(2)T	This command was on the Cisco 3600 series and the Cisco MC3810.

Usage Guidelines

The SGCP quarantine buffer is the mechanism for buffering the SGCP events between two notification-request (RQNT) messages.

Examples

The following example disables the SGCP quarantine buffer:

```
sgcp quarantine-buffer disable
```

Related Commands

Command	Description
sgcp	Starts and allocates resources for the SGCP daemon.
sgcp call-agent	Defines the IP address of the default SGCP call agent.
sgcp graceful-shutdown	Gracefully terminates all SGCP activity.
sgcp max-waiting-delay	Sets the SGCP maximum waiting delay to prevent restart avalanches.
sgcp modem passthru	Enables SGCP modem or fax pass-through.
sgcp request retries	Specifies the number of times to retry sending "notify" and "delete" messages to the SGCP call agent.
sgcp request timeout	Specifies how long the system should wait for a response to a request.

Command	Description
sgcp restart	Triggers the router to send an RSIP message to the SGCP call agent indicating that the T1 controller is up or down so that the call agent can synchronize with the T1 controller.
sgcp retransmit timer	Configures the SGCP retransmission timer to use a random algorithm method.
sgcp timer	Configures how the gateway detects the RTP stream host.
sgcp tse payload	Enables Inband TSE for fax/modem operation.

sgcp request retries

To specify the number of times to retry sending notify and delete messages to the Simple Gateway Control Protocol (SGCP) call agent, use the **sgcp request retries**command in global configuration mode. To reset to the default, use the **no** form of this command.

sgcp request retries *count*
no sgcp request retries

Syntax Description

count	Number of times that a notify and delete message is retransmitted to the SGCP call agent before it is dropped. Range is from 1 to 100. Default is 3.

Command Default

3 times

Command Modes

Global configuration (config)

Command History

Release	Modification
12.0(5)T	This command was introduced in a private release on the Cisco AS5300 and was not generally available.
12.0(7)XK	This command was implemented on the Cisco MC3810 and the Cisco 3600 series (except for the Cisco 3620) in a private release that was not generally available.
12.1(2)T	This command was implemented on the Cisco 3600 series and the Cisco MC3810.

Usage Guidelines

The actual retry count may be different from the value you enter for this command. The retry count is also limited by the call agent. If there is no response from the call agent after 30 seconds, the gateway does not retry anymore, even though the number set using the **sgcp request retries**command has not been reached.

The router stops sending retries after 30 seconds, regardless of the setting for this command.

Examples

The following example configures the system to send the **sgcp** command 10 times before dropping the request:

```
sgcp request retries 10
```

Related Commands

Command	Description
sgcp	Starts and allocates resources for the SGCP daemon.
sgcp call-agent	Defines the IP address of the default SGCP call agent.
sgcp graceful-shutdown	Gracefully terminates all SGCP activity.
sgcp max-waiting-delay	Sets the SGCP maximum waiting delay to prevent restart avalanches.
sgcp modem passthru	Enables SGCP modem or fax pass-through.

Command	Description
sgcp quarantine-buffer disable	Disables the SGCP quarantine buffer.
sgcp request timeout	Specifies how long the system should wait for a response to a request.
sgcp restart	Triggers the router to send an RSIP message to the SGCP call agent indicating that the T1 controller is up or down so that the call agent can synchronize with the T1 controller.
sgcp retransmit timer	Configures the SGCP retransmission timer to use a random algorithm method.
sgcp timer	Configures how the gateway detects the RTP stream host.
sgcp tse payload	Enables Inband TSE for fax/modem operation.

sgcp request timeout

To specify how long the system should wait for a response to a request, use the **sgcp request timeout**command in global configuration mode. To reset to the default, use the **no** form of this command.

sgcp request timeout *timeout*
no sgcp request timeout

Syntax Description

timeout	Time to wait for a response to a request, in milliseconds. Range is from 1 to 10000. Default is 500.

Command Default

500 ms

Command Modes

Global configuration (config)

Command History

Release	Modification
12.0(5)T	This command was introduced in a private release on the Cisco AS5300 and was not generally available.
12.0(7)XK	This command was implemented on the Cisco MC3810 and the Cisco 3600 series (except for the Cisco 3620) in a private release that was not generally available.
12.1(2)T	This command was implemented on the Cisco 3600 series and the Cisco MC3810.

Usage Guidelines

This command is used for "notify" and "delete" messages, which are sent to the SGCP call agent.

Examples

The following example configures the system to wait 40 ms for a reply to a request:

```
sgcp request timeout 40
```

Related Commands

Command	Description
sgcp	Starts and allocates resources for the SGCP daemon.
sgcp call-agent	Defines the IP address of the default SGCP call agent.
sgcp graceful-shutdown	Gracefully terminates all SGCP activity.
sgcp max-waiting-delay	Sets the SGCP maximum waiting delay to prevent restart avalanches.
sgcp modem passthru	Enables SGCP modem or fax pass-through.
sgcp quarantine-buffer disable	Disables the SGCP quarantine buffer.
sgcp request retries	Specifies the number of times to retry sending "notify" and "delete" messages to the SGCP call agent.

Command	Description
sgcp restart	Triggers the router to send an RSIP message to the SGCP call agent indicating that the T1 controller is up or down so that the call agent can synchronize with the T1 controller.
sgcp retransmit timer	Configures the SGCP retransmission timer to use a random algorithm method.
sgcp timer	Configures how the gateway detects the RTP stream host.
sgcp tse payload	Enables Inband TSE for fax/modem operation.

sgcp restart

To trigger the router to send a Restart in Progress (RSIP) message to the Simple Gateway Control Protocol (SGCP) call agent indicating that the T1 controller is up or down so that the call agent can synchronize with the T1 controller, use the **sgcp restart**command in global configuration mode. To reset to the default, use the **no** form of this command.

sgcp restart {**delay** *delay* | **notify**}
no sgcp restart {**delay** *delay* | **notify**}

Syntax Description

delay *delay*	Restart delay, in milliseconds. Range is from 0 to 600. Default is 0.
notify	Restarts notification upon the SGCP/digital interface state transition.

Command Default

0 ms

Command Modes

Global configuration(config)

Command History

Release	Modification
12.0(7)XK	This command was introduced on the Cisco MC3810 and the Cisco 3600 series (except the Cisco 3620) in a private release that was not generally available.
12.1(2)T	This command was implemented on the Cisco 3600 series and the Cisco MC3810.

Usage Guidelines

Use this command to send RSIP messages from the router to the SGCP call agent. RSIP messages are used to synchronize the router and the call agent. RSIP messages are also sent when the **sgcp** command is entered to enable the SGCP daemon.

You must enter the **notify** option to enable RSIP messages to be sent.

Examples

The following example configures the system to wait 40 ms before restarting SGCP:

```
sgcp restart delay 40
```

The following example configures the system to send an RSIP notification to the SGCP call agent when the T1 controller state changes:

```
sgcp restart notify
```

Related Commands

Command	Description
sgcp	Starts and allocates resources for the SGCP daemon.
sgcp call-agent	Defines the IP address of the default SGCP call agent.
sgcp graceful-shutdown	Gracefully terminates all SGCP activity.

Command	Description
sgcp max-waiting-delay	Sets the SGCP maximum waiting delay to prevent restart avalanches.
sgcp modem passthru	Enables SGCP modem or fax pass-through.
sgcp quarantine-buffer disable	Disables the SGCP quarantine buffer.
sgcp request retries	Specifies the number of times to retry sending "notify" and "delete" messages to the SGCP call agent.
sgcp request timeout	Specifies how long the system should wait for a response to a request.
sgcp retransmit timer	Configures the SGCP retransmission timer to use a random algorithm method.
sgcp timer	Configures how the gateway detects the RTP stream host.
sgcp tse payload	Enables Inband TSE for fax/modem operation.

sgcp retransmit timer

To configure the Simple Gateway Control Protocol (SGCP) retransmission timer to use a random algorithm, use the **sgcp retransmit timer**command in global configuration mode. To reset to the default, use the **no** form of this command.

sgcp retransmit timer random
no sgcp retransmit timer random

Syntax Description

random	SGCP retransmission timer uses a random algorithm.

Command Default

The SGCP retransmission timer does not use a random algorithm.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.0(7)XK	This command was introduced on the Cisco 3600 series and the Cisco MC3810 in a private release that was not generally available.
12.1(2)T	This command was implemented on the Cisco 3600 series and the Cisco MC3810.

Usage Guidelines

Use this command to enable the random algorithm component of the retransmission timer. For example, if the retransmission timer is set to 200 ms, the first retransmission timer is 200 ms, but the second retransmission timer picks up a timer value randomly between either 200 or 400. The third retransmission timer picks up a timer value randomly of 200, 400, or 800 as shown below:

- First retransmission timer: 200
- Second retransmission timer: 200 or 400
- Third retransmission timer: 200, 400, or 800
- Fourth retransmission timer: 200, 400, 800, or 1600
- Fifth retransmission timer: 200, 400, 800, 1600, or 3200 and so on.

After 30 seconds, the retransmission timer no longer retries.

Examples

The following example sets the retransmission timer to use a random algorithm:

```
sgcp retransmit timer random
```

Related Commands

Command	Description
sgcp	Starts and allocates resources for the SGCP daemon.
sgcp call-agent	Defines the IP address of the default SGCP call agent.

Command	Description
sgcp graceful-shutdown	Gracefully terminates all SGCP activity.
sgcp max-waiting-delay	Sets the SGCP maximum waiting delay to prevent restart avalanches.
sgcp modem passthru	Enables SGCP modem or fax pass-through.
sgcp quarantine-buffer disable	Disables the SGCP quarantine buffer.
sgcp request retries	Specifies the number of times to retry sending "notify" and "delete" messages to the SGCP call agent.
sgcp request timeout	Specifies how long the system should wait for a response to a request.
sgcp restart	Triggers the router to send an RSIP message to the SGCP call agent indicating that the T1 controller is up or down so that the call agent can synchronize with the T1 controller.
sgcp timer	Configures how the gateway detects the RTP stream host.
sgcp tse payload	Enables Inband TSE for fax/modem operation.

sgcp timer

To configure how the gateway detects the Real-Time Transport Protocol (RTP) stream lost, use the **sgcp timer**command in global configuration mode. To reset to the default, use the **no** form of this command.

sgcp timer {**receive-rtcp** *timer* | **rtp-nse** *timer*}
no sgcp timer {**receive-rtcp** *timer* | **rtp-nse** *timer*}

Syntax Description

receive -rtcp *timer*	RTP Control Protocol (RTCP) transmission interval, in milliseconds. Range is from 1 to 100. Default is 5.
rtp -nse *timer*	RTP named signaling event (NSE) timeout, in milliseconds. Range is from 100 to 3000. Default is 200.

Command Default

receive -rtcp: 5 ms

rtp -nse: 200 ms

Command Modes

Global configuration (config)

Command History

Release	Modification
12.0(5)T	This command was introduced in a private release on the Cisco AS5300 and was not generally available.
12.0(7)XK	This command was implemented on the Cisco MC3810 and the Cisco 3600 series (except for the Cisco 3620) in a private release that was not generally available.
12.1(2)T	This command was implemented on the Cisco 3600 series and the Cisco MC3810.

Usage Guidelines

The RTP NSE timer is used for proxy ringing (the ringback tone is provided at the originating gateway).

Examples

The following example sets the RTPCP transmission interval to 100 ms:

```
sgcp timer receive-rtcp 100
```

The following example sets the NSE timeout to 1000 ms:

```
sgcp timer rtp-nse 1000
```

Related Commands

Command	Description
sgcp	Starts and allocates resources for the SGCP daemon.
sgcp call-agent	Defines the IP address of the default SGCP call agent.
sgcp graceful-shutdown	Gracefully terminates all SGCP activity.

Command	Description
sgcp max-waiting-delay	Sets the SGCP maximum waiting delay to prevent restart avalanches.
sgcp modem passthru	Enables SGCP modem or fax pass-through.
sgcp quarantine-buffer disable	Disables the SGCP quarantine buffer.
sgcp request retries	Specifies the number of times to retry sending "notify" and "delete" messages to the SGCP call agent.
sgcp request timeout	Specifies how long the system should wait for a response to a request.
sgcp restart	Triggers the router to send an RSIP message to the SGCP call agent indicating that the T1 controller is up or down so that the call agent can synchronize with the T1 controller.
sgcp retransmit timer	Configures the SGCP retransmission timer to use a random algorithm method.
sgcp tse payload	Enables Inband TSE for fax/modem operation.

sgcp tse payload

To enable Inband Telephony Signaling Events (TSE) for fax and modem operation, use the **sgcp tse payload**command in global configuration mode. To reset to the default, use the **no** form of this command.

sgcp tse payload *type*
no sgcp tse payload *type*

Syntax Description

type	TSE payload type. Range is from 96 to 119. Default is 0, meaning that the command is disabled.

Command Default

0 (disabled)

Command Modes

Global configuration(config)

Command History

Release	Modification
12.0(7)XK	This command was introduced on the Cisco MC3810 and the Cisco 3600 series (except the Cisco 3620) in a private release that was not generally available.
12.1(2)T	This command was implemented on the Cisco 3600 series and the Cisco MC3810.

Usage Guidelines

Because this command is disabled by default, you must specify a TSE payload type.

If you set the **sgcp modem passthru** command to the **nse** value, then you must configure this command.

Examples

The following example sets Simple Gateway Control Protocol (SGCP) modem pass-through using the NSE-based modem upspeed and the Inband Telephony Signaling Events payload value set to 110:

```
sgcp modem passthru nse
sgcp tse payload 110
```

Related Commands

Command	Description
sgcp	Starts and allocates resources for the SGCP daemon.
sgcp call-agent	Defines the IP address of the default SGCP call agent.
sgcp graceful-shutdown	Gracefully terminates all SGCP activity.
sgcp max-waiting-delay	Sets the SGCP maximum waiting delay to prevent restart avalanches.
sgcp modem passthru	Enables SGCP modem or fax pass-through.
sgcp quarantine-buffer disable	Disables the SGCP quarantine buffer.
sgcp request retries	Specifies the number of times to retry sending "notify" and "delete" messages to the SGCP call agent.

Command	Description
sgcp request timeout	Specifies how long the system should wait for a response to a request.
sgcp restart	Triggers the router to send an RSIP message to the SGCP call agent indicating that the T1 controller is up or down so that the call agent can synchronize with the T1 controller.
sgcp retransmit timer	Configures the SGCP retransmission timer to use a random algorithm method.up or down so that the call agent can synchronize
sgcp timer	Configures how the gateway detects the RTP stream host.

source filter

To filter Real-time Transport Protocol (RTP) packets with a source IP address and port number that are different from the one negotiated through Session Initiation Protocol (SIP) signaling, use the **source filter** command in voice service SIP configuration mode. To disable filtering, use the **no** form of this command.

source filter
no source filter

Command Default

RTP source filtering is disabled.

Command Modes

Voice service SIP configuration (conf-serv-sip)

Command History

Release	Modification
12.4(6)T	This command was introduced.

Usage Guidelines

Public Switched Telephone Network (PSTN) callers may experience crosstalk when the SIP IOS gateway receives an invalid RTP stream destined to the same IP address and port of an active call. The invalid stream has a different source IP address and port than the one negotiated using SIP Session Description Protocol (SDP). The Digital Signal Processor (DSP) within the gateway mixes both the valid and invalid RTP streams and plays it to the PSTN caller. Use the **source filter** command when you want to filter RTP packets with a source IP address and port number that are different from the one negotiated through SIP signaling.

Examples

The following example shows how to filter RTP packets:

```
Device> enable
Device# configure terminal
Device(config)# voice service voip
Device(conf-voi-serv)# sip
Device(conf-serv-sip)# source filter
```

Related Commands

Command	Description
sip	Enters SIP configuration mode.
voice service voip	Specifies the voice-encapsulation type and enters voice service configuration mode.



show aal2 profile through show call filter match-list

- show aal2 profile, on page 168
- show app-hosting detail, on page 170
- show atm video-voice address, on page 172
- show auto-config, on page 173
- show backhaul-session-manager group, on page 175
- show backhaul-session-manager session, on page 178
- show backhaul-session-manager set, on page 180
- show call accounting-template voice, on page 181
- show call active fax, on page 184
- show call active media, on page 194
- show call active total-calls, on page 202
- show call active video, on page 203
- show call active voice, on page 214
- show call application app-level, on page 237
- show call application gateway-level, on page 241
- show call application interface, on page 244
- show call application services registry, on page 248
- show call application session-level, on page 250
- show call application sessions, on page 262
- show call application voice, on page 265
- show call fallback cache, on page 271
- show call fallback config, on page 273
- show call fallback stats, on page 275
- show call filter components, on page 277
- show call filter match-list, on page 279

show aal2 profile

To display the ATM adaptation layer 2 (AAL2) profiles configured on the system, use the **show aal2 profile** command in privileged EXEC mode.

show aal2 profile all {**itut** *profile-number* | **atmf** *profile-number* | **custom** *profile-number*}

Syntax Description

all	Displays ITU-T, ATMF, and custom AAL2 profiles configured on the system.
itut	Displays ITU-T profiles configured on the system.
atmf	Displays ATMF profiles configured on the system.
custom	Displays custom profiles configured on the system.
profile -number	AAL2 profile number to display. Choices are as follows: For ITU-T: • 1 = G.711 u-law • 2 = G.711 u-law with silence insertion descriptor (SID) • 7 = G.711 u-law and G.729ar8 For ATMF: None. ATMF is not supported. For custom: • 100 = G.711 u-law and G.726r32 • 110 = G.711 u-law, G.726r32, and G.729ar8

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.1(1)XA	This command was introduced on the Cisco MC3810.
12.1(2)T	This command was integrated into Cisco IOS Release 12.1(2)T.
12.2(2)T	This command was implemented on the Cisco 7200 series.

Usage Guidelines

This command applies to AAL2 VoATM applications on the Cisco 7200 series routers.

Examples

The following command displays all of the configured profiles in the system:

```
Router# show aal2 profile all
Printing all the Profiles in the system
Profile Type: ITUT Profile Number: 1 SID Support: 0
Red enable: 1 Num entries: 1
```

```
Coding type: g711ulaw Packet length: 40 UUI min: 0 UUI max: 15
Profile Type: ITUT Profile Number: 2 SID Support: 1
Red enable: 1 Num entries: 1
Coding type: g711ulaw Packet length: 40 UUI min: 0 UUI max: 15
Profile Type: custom Profile Number: 100 SID Support: 1
Red enable: 1 Num entries: 2
Coding type: g711ulaw Packet length: 40 UUI min: 0 UUI max: 7
Coding type: g726r32 Packet length: 40 UUI min: 8 UUI max: 15
Profile Type: ITUT Profile Number: 7 SID Support: 1
Red enable: 1 Num entries: 2
Coding type: g711ulaw Packet length: 40 UUI min: 0 UUI max: 15
Coding type: g729ar8 Packet length: 10 UUI min: 0 UUI max: 15
Profile Type: custom Profile Number: 110 SID Support: 1
Red enable: 1 Num entries: 3
Coding type: g711ulaw Packet length: 40 UUI min: 0 UUI max: 7
Coding type: g726r32 Packet length: 40 UUI min: 8 UUI max: 15
Coding type: g729ar8 Packet length: 30 UUI min: 8 UUI max: 15
```

The table below describes significant fields shown in this output.

Table 7: show aal2 profile all Field Descriptions

Field	Description
Coding type	Voice compression algorithm.
ITUT Profile Number	Predefined combination of one or more codec types configured for a digital signal processor (DSP).
Num entries	Number of profile elements.
Packet length	Sample size.
Profile Type	Category of codec types configured on DSP. Possible types are ITU-T, ATMF, and custom.
Red enable	Redundancy for type 3 packets.
SID Support	Silence insertion descriptor.
UUI max	Maximum sequence number on the voice packets.
UUI min	Minimum sequence number on the voice packets.

Related Commands

Command	Description
codec aal2-profile	Sets the codec profile for a DSP on a per-call basis.

show app-hosting detail

To view detailed information about a specific hosted application (container or virtualized application) on a Cisco IOS XE device, use the **show app-hosting detail** command in privileged EXEC mode.

show app-hosting detail appid *application_id*

Syntax Description

appid *application_id*	This specifies the unique identifier (App ID) of the application for which you want to see the details.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Fuji 16.12.1	This command was introduced.

Usage Guidelines

Output of the **show app-hosting detail** command typically includes Application State, Application Type, Resource Reservations, Network Configuration, File Locations, and Version Information.

Examples

The following is an example for **show app-hosting detail appid vdsp** command. Observe that the vDSP container is in RUNNING state:

```
router# show app-hosting detail appid vdsp
App id : vdsp
Owner : iox
State : RUNNING
Application
Type : docker
Name : vDSP-DSPFARM-Feature
Version : 1.0.827
Description : Built on 2024-08-27 21:58:36
Author : Cisco Systems, Inc.
Path : bootflash:vDSP_1.0.827.aarch64.tar
URL Path :
Activated profile name : vDSP-500
Resource reservation
Memory : 1010 MB
Disk : 256 MB
CPU : 11495 units
CPU-percent : 34 %
VCPU : 1
Platform resource profiles
Profile Name CPU(unit) CPU(percent) Memory(MB) Disk(MB)
--------------------------------------------------------------------------------
vDSP-50         17         --        1001       256
vDSP-100        17         --        1002       256
...
Docker
------
Run-time information
Command :
Entry-point : /root/vdsp_start.sh
Run options in use :
```

```
Package run options :
Application health information
Status : 0
Last probe error :
Last probe output : 6.2 0.0 0.0 0.0 0.0 6.2 41
```

show atm video-voice address

To display the network service access point (NSAP) address for the ATM interface, enter the **show atm video-voice address**command inprivileged EXEC mode.

show atm video-voice address

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.0(5)XK	This command was introduced on the Cisco MC3810.
12.0(7)T	This command was integrated into Cisco IOS Release 12.0(7)T.

Usage Guidelines

Use this command to review ATM interface NSAP addresses that have been assigned with the atm video aesa command and to ensure that ATM management is confirmed for those addresses.

Examples

The following example displays ATM interface NSAP addresses:

```
Router# show atm video-voice address
nsap address                                    type         ilmi status
47.0091810000000002F26D4901.00107B4832E1.FE   VOICE_AAL5   Confirmed
47.0091810000000002F26D4901.00107B4832E1.C8   VIDEO_AAL1   Confirmed
```

The table below describes the significant fields shown in the output.

Table 8: show atm video-voice address Field Descriptions

Field	Description
NSAP address	NSAP address for the ATM interface.
Type	Type of ATM interface.
ILMI status	Integrated Local management Interface (ILMI) protocol status for the ATM interface.

Related Commands

Command	Description
codec aal2-profile	Sets the codec profile for a DSP on a per-call basis.

show auto-config

To display the current status of auto-configuration applications, use the **show auto-config**command in privileged EXEC mode.

show auto-config [**application sccp**]

Syntax Description

application sccp	Displays the current status of only the Skinny Client Control Protocol (SCCP) application.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.3(8)XY	This command was introduced on the Communication Media Module.
12.3(14)T	This command was integrated into Cisco IOS Release 12.3(14)T.

Examples

The following is sample output from **show auto-config** command:

```
Router# show auto-config application sccp
 auto-config application: sccp
 auto-config admin state: ENABLED & ACTIVE
 download retries: (3)
 download timeout: no timeout, continuous retry
 server(s):  172.19.240.41 172.19.240.40 172.19.240.42
Configuration Download statistics:
        Download Attempted             : 2
          Download Successful          : 2
          Download Failed              : 0
        Configuration Attempted        : 2
          Configuration Successful     : 2
          Configuration Failed(parsing): 0
          Configuration Failed(config) : 0
Configuration Error History:
```

The table below describes the significant fields shown in the display.

Table 9: show auto-config Field Descriptions

Field	Description
ENABLED	Shows auto-config application: SCCP is enabled.
ACTIVE	Shows the SCCP application has registered to use auto-configuration.
timeout	Shows timeout is set to 0, continuous retry without timeout.

Related Commands

Command	Description
auto-config	Enables auto-configuration or enters auto-config application configuration mode for the SCCP application.
debug auto-config	Enables debugging for auto-configuration applications.
debug sccp config	Enables SCCP event debugging.

show backhaul-session-manager group

To display the status, statistics, or configuration for a particular session group or all available session groups, use the **show backhaul-session-manager group**command in privileged EXEC mode.

show backhaul-session-manager group {**status** | **stats** | **cfg**} {**all** | **name** *group-name*}

Syntax Description

status	Status for available session groups.
stats	Statistics for available session groups.
cfg	Configuration for available session groups.
all	Specified parameters for all session groups.
name *group -name*	A particular session group.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.1(1)T	This command was introduced on the Cisco AS5300.
12.2(2)T	This command was implemented on the Cisco 7200 series.
12.2(4)T	This command was implemented on the Cisco 2600 series, Cisco 3600 series, and Cisco MC3810.
12.2(2)XB	This command was implemented on the Cisco AS5350 and Cisco AS5400.
12.2(2)XB1	This command was implemented on the Cisco AS5850.
12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T and was implemented on the Cisco IAD2420 series. Support for the Cisco AS5300, Cisco AS5350, Cisco AS5400, and Cisco AS5850 is not included in this release.
12.2(11)T	This command is supported on the Cisco AS5300, Cisco AS5350, Cisco AS5400, and Cisco AS5850 in this release.

Examples

The following example displays statistics for all session groups:

```
Router# show backhaul-session-manager group stats all
Session-Group grp1 statistics
   Successful Fail-Overs      :0
   Un-Successful Fail-Over attempts:0
   Active Pkts receive count  :0
   Standby Pkts receive count :0
   Total PDUs dispatch err    :0
```

The following example displays the current configuration for all session groups:

```
Router# show backhaul-session-manager group cfg all
Session-Group
   Group Name :grp1
   Set Name   :set1
   Sessions   :3
    Dest:10.5.0.3 8304  Local:10.1.2.15 8304  Priority:0
    Dest:10.5.0.3 8300  Local:10.1.2.15 8300  Priority:2
    Dest:10.5.0.3 8303  Local:10.1.2.15 8303  Priority:2
    RUDP Options
      timer cumulative ack :100
      timer keepalive      :1000
      timer retransmit     :300
      timer transfer state :2000
      receive max          :32
      cumulative ack max   :3
      retrans max          :2
      out-of-sequence max  :3
      auto-reset max       :5
```

The following example displays the current state of all session groups. The group named "grp1" belongs to the set named "set1".

```
Router# show backhaul-session-manager group status all
Session-Group
Group Name   :grp1
   Set Name     :set1
   Status       :Group-OutOfService
   Status (use) :Group-None
```

The table below describes the significant fields shown in the output.

Table 10: show backhaul-session-manager group Field Descriptions

Field	Descrption
RUDP Options	Reliable User datagram Protocol (RUDP) options.
Status	One of the following: • Group-OutOfService--No session in the group has been established. • Group-Inservice--At least one session in the group has been established.
Status (use)	One of the following: • Group-Standby--The virtual switch controller (VSC) connected to the other end of this group goes into standby mode. • Group-Active--The VSC connected to the other end of this group is the active VSC. • Group-None--The VSC has not yet declared its intent.

Related Commands

Command	Description
show backhaul-session-manager session	Displays status, statistics, or configuration of sessions.

Command	Description
show backhaul-session-manager set	Displays session groups associated with a specific session set or all session sets.

show backhaul-session-manager session

To display various information about a session or sessions, use the **show backhaul-session-manager session** command in privileged EXEC mode.

show backhaul-session-manager session {**all** | **ip** *ip-address*}

Syntax Description

all	Information is displayed about all available sessions.
ip	Information is displayed about the session associated with this IP address only.
ip -address	IP address of the local or remote session.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.1(1)T	This command was introduced on the Cisco AS5300.
12.2(2)T	This command was implemented on the Cisco 7200 series.
12.2(4)T	This command was implemented on the Cisco 2600 series, Cisco 3600 series, and Cisco MC3810.
12.2(2)XB	This command was implemented on the Cisco AS5350 and Cisco AS5400.
12.2(2)XB1	This command was implemented on the Cisco AS5850.
12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T and was implemented on the Cisco IAD2420 series. Support for the Cisco AS5350, Cisco AS5400, and Cisco AS5850 is not included in this release.
12.2(11)T	This command was implemented on the Cisco AS5350, Cisco AS5400, and Cisco AS5850.

Examples

The following command displays information for all available sessions:

```
Router# show backhaul-session-manager session all
Session information --
Session-id:35
  Group:grp1  /*this session belongs to the group named 'grp1' */
Configuration:
     Local:10.1.2.15      , port:8303
    Remote:10.5.0.3       , port:8303
  Priority:2
  RUDP Option:Client, Conn Id:0x2
State:
  Status:OPEN_WAIT, Use-status:OOS,  /*see explanation below */
Statistics:
  # of resets:0
  # of auto_resets 0
  # of unexpected RUDP transitions (total) 0
```

```
  # of unexpected RUDP transitions (since last reset) 0
  Receive pkts -  Total:0 , Since Last Reset:0
  Recieve failures -  Total:0 ,Since Last Reset:0
  Transmit pkts - Total:0, Since Last Reset:0
  Transmit Failures (PDU Only)
         Due to Blocking (Not an Error) - Total:0, Since Last Reset:0
         Due to causes other than Blocking - Total:0, Since Last
Reset:0
  Transmit Failures (NON-PDU Only)
         Due to Blocking(Not an Error) - Total:0, Since Last Reset:0
         Due to causes other than Blocking - Total:0, Since Last
Reset:0
  RUDP statistics
         Open failures:0
         Not ready failures:0
         Conn Not Open failures:0
         Send window full  failures:0
         Resource unavailble failures:0
         Enqueue failures:0
```

The table below describes significant fields shown in this output.

Table 11: show backhaul-session-manager session Field Descriptions

Field	Description
State	Can be any of the following: • OPEN--The connection is established. • OPEN_WAIT--The connection is awaiting establishment. • OPEN_XFER--Session failover is in progress for this session, which is a transient state. • CLOSE--The session is down, also a transient state. The session waits a fixed amount of time and then moves to OPEN_WAIT.
Use-status	Indicates whether PRI signaling traffic is currently being transported over this session. Can be either of the following: • OOS--The session is not being used to transport signaling traffic. Out of service (OOS) does not indicate if the connection is established. • IS--The session is being used currently to transport all PRI signaling traffic. In service (IS) indicates that the connection is established.

Related Commands

Command	Description
show backhaul-session-manager group	Displays status, statistics, or configuration of a specific session group or all session groups.
show backhaul-session-manager set	Displays session groups associated with a specific session set or all session sets.

show backhaul-session-manager set

To display session groups associated with a specified session set or all session sets, use the **show backhaul-session-manager set**command in privileged EXEC mode.

show backhaul-session-manager set {**all** | **name** *session-set-name*}

Syntax Description

all	All available session sets.
name *session -set -name*	A specified session set.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.1(1)T	This command was introduced on the Cisco AS5300.
12.2(2)T	This command was implemented on the Cisco 7200 series.
12.2(4)T	This command was implemented on the Cisco 2600 series, Cisco 3600 series, and Cisco MC3810.
12.2(2)XB	This command was implemented on the Cisco AS5350 and Cisco AS5400.
12.2(2)XB1	This command was implemented on the Cisco AS5850.
12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T and was implemented on the Cisco IAD2420 series. Support for the Cisco AS5350, Cisco AS5400, and Cisco AS5850 is not included in this release.
12.2(11)T	This command is supported on the Cisco AS5350, Cisco AS5400, and Cisco AS5850 in this release.

Examples

The following command displays session groups associated with all session sets:

```
Router# show backhaul-session-manager set all
```

Related Commands

Command	Description
show backhaul -session-manager group	Displays status, statistics, or configuration of a specific session group or all session groups.
show backhaul -session-manager session	Displays status, statistics, or configuration of a session or all sessions.

show call accounting-template voice

To display accounting template activity, use the **show call accounting-template voice** command in privileged EXEC mode.

show call accounting-template voice [*WORD* | **attrList** | **qdump** | **summary**]

Syntax Description

WORD	(Optional) Name of the accounting template.
attrList	(Optional) Displays all vendor-specific attributes (VSAs) that are filtered by accounting templates.
qdump	(Optional) Displays template activity in the service and free queues.
summary	(Optional) Lists names of all the accounting templates and the number of attributes in each template currently being used.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.2(11)T	This command was introduced on the Cisco 3660, Cisco AS5300, Cisco AS5350, Cisco AS5400, Cisco AS5800, and Cisco AS5850.

Usage Guidelines

- The **show call accounting-template voice** command displays the status and attributes defined in each template after it is configured.
- The **show call accounting-template voice** *WORD* command displays the status of a specific template and the attributes (VSAs) that are defined for that template.
- The **show call accounting-template voice attrList** command displays all VSAs that can be filtered by accounting templates.
- The **show call accounting-template voice qdump** command displays template activity in the service (svc) and free queues. It displays the template URL, the number of legs on which a template is active, and the state of a template.
  - After an accounting template is defined, it is put in the svc queue to serve new incoming calls. When a running accounting template is undefined or reloaded during an active call, the template is moved from the svc queue to the free queue and can be reused after all the active calls stop referencing it. Templates that are reloaded or undefined and that are referenced during an active call are considered to be in a "dirty" state and are called dirty templates.
  - To ensure that start and stop records correspond on an active call that is referencing a dirty template, all dirty templates must be kept alive until all active calls referencing that dirty template are released. After all active calls are released, the reloaded templates are applied to the next call.
- The **show call accounting-template voice summary** command displays the current status of all the accounting templates that are configured. It shows if the template was loaded and if it is running successfully.

Examples

The following example displays details about two templates named "cdr1" and "cdr2".

```
Router# show call accounting-template voice
CDR template cdr1 is running
url: tftp://sanjoe/santa/abc/Templates/cdr1.cdr
The last load was successful.
attr:  h323-call-origin (56)
attr:  h323-call-type (57)
attr:  h323-gw-id (65)
attr:  subscriber (79)
attr:  in-portgrp-id (80)
attr:  out-portgrp-id (81)
Totally 6 attrs defined.
CDR template cdr2 is running
url: tftp://sanjoe/santa/abc/Templates/cdr2.cdr
The last load was successful.
attr:  h323-call-origin (56)
attr:  h323-call-type (57)
attr:  h323-connect-time (59)
attr:  h323-disconnect-time (64)
attr:  h323-gw-id (65)
attr:  h323-setup-time (76)
attr:  h323-voice-quality (78)
Totally 7 attrs defined.
```

The following example displays details about the template named "cdr1" only.

```
Router# show call accounting-template voice cdr1
CDR template cdr1 is running
url: tftp://sanjoe/santa/abc/Templates/cdr1.cdr
The last load was successful.
attr:  h323-call-origin (56)
attr:  h323-call-type (57)
attr:  h323-gw-id (65)
attr:  subscriber (79)
attr:  in-portgrp-id (80)
attr:  out-portgrp-id (81)
Totally 6 attrs defined.
```

The following example displays all 64 attributes that can be filtered by a template.

```
Router# show call accounting-template voice attrList
h323-call-origin
h323-call-type
h323-gw-id
h323-setup-time
h323-connect-time
h323-disconnect-time
h323-disconnect-cause
.
.
.
calling-party-category
originating-line-info
charge-number
transmission-medium-req
redirecting-number
backward-call-indicators
Totally 64 attributes are filterable.
```

The following example displays template activity in the service queue. Initially, no templates are in the dirty state.

```
Router# show call accounting-template voice qdump
name         url                                 is_dirty   no_of_legs
=============================================================================
cdr1         tftp://sanjoe/santa/abc                        0
cdr2         tftp://sanjoe/santa/abc                        0
cdr3         tftp://sanjoe/santa/abc                        0
```

After the templates are reloaded during active calls, the display below shows the templates named "cdr1" and "cdr2" to be in a dirty state.

```
.
.
.
Templates in freeq
cdr1         tftp://sanjoe/santa/abc            dirty       1
cdr2         tftp://sanjoe/santa/abc            dirty       1
```

The following example displays a summary of all configured accounting templates. The template named "cdr3" is not in running mode, either because it has been rejected or because it does not exist at the given URL.

```
Router# show call accounting-template voice summary
name         url                                       last_load  is_running
=============================================================================
cdr1         tftp://sanjoe/santa/abc                   success    is running
cdr2         tftp://sanjoe/santa/abc                   success    is running
cdr3         tftp://sanjoe/santa/abc                   fail       is not running
```

The table below describes the fields shown in the **show call accounting-template voice** display.

Table 12: show call accounting-template voice Field Descriptions

Field	Description
name	Name of the accounting template.
url	Location of the accounting template.
last_load	Describes if the accounting template was successfully or unsuccessfully loaded from its location.
is_running	Describes if the accounting template was activated after it was successfully loaded from its location.
is_dirty	Shows that the accounting template was reloaded during an active call.
no_of_legs	Number of call legs.
attr	Vendor-specific attributes (VSAs) defined in an accounting template.

Related Commands

Command	Description
gw-accounting aaa	Configures a new accounting template.

show call active fax

To display call information for T.37 store-and-forward fax transmissions in progress, use the **show call active fax** command in user EXEC or privileged EXEC mode.

show call active fax [**brief** [**id** *identifier*] | **compact** [**duration** {**less** *seconds* | **more** *seconds*}] | **id** *identifier*]

Syntax Description

brief	(Optional) Displays a truncated version of fax call information.
id *identifier*	(Optional) Displays only the call with the specified *identifier* . Range is a hex value from 1 to FFFF.
compact	(Optional) Displays a compact version of the fax call information.
duration	(Optional) Displays active calls that are longer or shorter than a specified *seconds* value. The arguments and keywords are as follows: • **less** --Displays calls shorter than the *seconds* value. • **more** --Displays calls longer than the *seconds* value. • *seconds* --Elapsed time, in seconds. Range is from 1 to 2147483647. There is no default value.

Command Modes

User EXEC (>)
Privileged EXEC (#)

Command History

Release	Modification
11.3(1)T	This command was introduced on the Cisco 2600 series and Cisco 3600 series.
12.0(3)XG	This command was modified. Support for Voice over Frame Relay (VoFR) was added.
12.0(4)XJ	This command was implemented for store-and-forward fax on the Cisco AS5300.
12.0(4)T	This command was implemented on the Cisco 7200 series.
12.0(7)XK	This command was implemented on the Cisco MC3810.
12.1(2)T	This command was integrated into Cisco IOS Release 12.1(2)T.
12.1(3)T	This command was modified. This command was implemented for modem pass-through over VoIP on the Cisco AS5300.
12.1(5)XM	This command was implemented on the Cisco AS5800.
12.1(5)XM2	The command was implemented on the Cisco AS5350 and Cisco AS5400.
12.2(2)XB1	This command was implemented on the Cisco AS5850.

Release	Modification
12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T. Support was not included for the Cisco AS5300, Cisco AS5350, Cisco AS5400, and Cisco AS5850.
12.2(11)T	Support was added for the Cisco AS5300, Cisco AS5350, Cisco AS5400, and Cisco AS5850.
12.3(14)T	This command was modified. T.38 fax relay call statistics were made available to Call Detail Records (CDRs) through vendor-specific attributes (VSAs) and added to the call log.
12.4(2)T	This command was modified. The LocalHostname display field was added to the VoIP call leg record.
12.4(15)T	This command was modified. The Port and BearerChannel display fields were added to the TELE call leg record of the command output.
12.4(16)	This command was modified. The Port and BearerChannel display fields were added to the TELE call leg record of the command output.
12.4(22)T	This command was modified. Command output was updated to show IPv6 information.

Usage Guidelines

Use this command to display the contents of the active call table. This command displays information about call times, dial peers, connections, quality of service, and other status and statistical information for T.37 store-and-forward fax calls currently connected through the router. This command works with both on-ramp and off-ramp store-and-forward fax functions.

To display information about fax relay calls in progress, use the **show call active voice** command.

Examples

The following is sample output from the **show call active fax** command:

```
Router# show call active fax
GENERIC:
SetupTime=22021 ms
Index=1
PeerAddress=peer one
PeerSubAddress=
PeerId=0
PeerIfIndex=0
LogicalIfIndex=0
ConnectTime=24284
CallState=4
CallOrigin=2
ChargedUnits=0
InfoType=10
TransmitPackets=0
TransmitBytes=0
ReceivePackets=0
ReceiveBytes=41190
MMOIP:
ConnectionId[0x37EC7F41 0xB0110001 0x0 0x35C34]
CallID=1
RemoteIPAddress=10.0.0.0
SessionProtocol=SMTP
SessionTarget=
MessageId=
AccountId=
ImgEncodingType=MH
```

```
ImgResolution=fine
AcceptedMimeTypes=2
DiscardedMimeTypes=1
Notification=None
GENERIC:
SetupTime=23193 ms
Index=1
PeerAddress=527....
PeerSubAddress=
PeerId=3469
PeerIfIndex=157
LogicalIfIndex=30
ConnectTime=24284
CallState=4
CallOrigin=1
ChargedUnits=0
InfoType=10
TransmitPackets=5
TransmitBytes=6513
ReceivePackets=0
ReceiveBytes=0
TELE:
ConnectionId=[0x37EC7F41 0xB0110001 0x0 0x35C34]
CallID=2
Port=3/0/0 (2)
BearerChannel=3/0/0.1
TxDuration=24010 ms
FaxTxDuration=10910 ms
FaxRate=14400
NoiseLevel=-1
ACOMLevel=-1
OutSignalLevel=0
InSignalLevel=0
InfoActivity=0
ERLLevel=-1
SessionTarget=
ImgPages=0
```

The table below provides an alphabetical listing of the fields displayed in the output of the **show call active fax**command and a description of each field.

Table 13: show call active fax Field Descriptions

Field	Description
ACOM Level	Current ACOM level for this call. ACOM is the combined loss achieved by the echo canceler, which is the sum of the Echo Return Loss, Echo Return Loss Enhancement, and nonlinear processing loss for the call.
BearerChannel	Identification of the bearer channel carrying the call.
Buffer Drain Events	Total number of jitter buffer drain events.
Buffer Fill Events	Total number of jitter buffer fill events.
CallDuration	Length of the call, in hours, minutes, and seconds, hh:mm:ss.
CallOrigin	Call origin: answer or originate.
CallState	Current state of the call.

Field	Description
ChargedUnits	Total number of charging units that apply to this peer since system startup. The unit of measure for this field is hundredths of second.
CodecBytes	Payload size, in bytes, for the codec used.
CoderTypeRate	Negotiated coder rate. This value specifies the send rate of voice or fax compression to its associated call leg for this call.
ConnectionId	Global call identifier for this gateway call.
ConnectTime	Time, in milliseconds, at which the call was connected.
Consecutive-packets-lost Events	Total number of consecutive (two or more) packet-loss events.
Corrected packet-loss Events	Total number of packet-loss events that were corrected using the RFC 2198 method.
Dial-Peer	Tag of the dial peer sending this call.
EchoCancellerMaxReflector=64	The location of the largest reflector, in milliseconds (ms). The reflector size does not exceed the configured echo path capacity. For example, if 32 ms is configured, the reflector does not report beyond 32 ms.
ERLLevel	Current echo return loss (ERL) level for this call.
FaxTxDuration	Duration of fax transmission from this peer to the voice gateway for this call. You can derive the Fax Utilization Rate by dividing the FaxTxDuration value by the TxDuration value.
GapFillWithInterpolation	Duration of a voice signal played out with a signal synthesized from parameters, or samples of data preceding and following in time because voice data was lost or not received in time from the voice gateway for this call.
GapFillWithPrediction	Duration of the voice signal played out with signal synthesized from parameters, or samples of data preceding in time, because voice data was lost or not received in time from the voice gateway for this call. Examples of such pullout are frame-eraser and frame-concealment strategies in G.729 and G.723.1 compression algorithms.
GapFillWithRedundancy	Duration of a voice signal played out with a signal synthesized from available redundancy parameters because voice data was lost or not received in time from the voice gateway for this call.
GapFillWithSilence	Duration of a voice signal replaced with silence because voice data was lost or not received in time for this call.
GENERIC	Generic or common parameters, that is, parameters that are common for VoIP and telephony call legs.
H323 call-legs	Total H.323 call legs for which call records are available.
HiWaterPlayoutDelay	High-water-mark Voice Playout FIFO Delay during this call, in ms.

Field	Description
Index	Dial peer identification number.
InfoActivity	Active information transfer activity state for this call.
InfoType	Information type for this call; for example, voice or fax.
InSignalLevel	Active input signal level from the telephony interface used by this call.
Last Buffer Drain/Fill Event	Elapsed time since the last jitter buffer drain or fill event, in seconds.
LocalHostname	Local hostnames used for locally generated gateway URLs.
LogicalIfIndex	Index number of the logical interface for this call.
LoWaterPlayoutDelay	Low-water-mark Voice Playout FIFO Delay during this call, in ms.
LowerIFName	Physical lower interface information. Appears only if the medium is ATM, Frame Relay (FR), or High-Level Data Link Control (HDLC).
Media	Medium over which the call is carried. If the call is carried over the (telephone) access side, the entry is TELE. If the call is carried over the voice network side, the entry is either ATM, FR, or HDLC.
Modem passthrough signaling method in use	Indicates that this is a modem pass-through call and that named signaling events (NSEs)--a Cisco-proprietary version of named telephone events in RFC 2833--are used for signaling codec upspeed. The upspeed method is the method used to dynamically change the codec type and speed to meet network conditions. This means that you might move to a faster codec when you have both voice and data calls and then slow down when there is only voice traffic.
NoiseLevel	Active noise level for this call.
OnTimeRvPlayout	Duration of voice playout from data received on time for this call. Derive the Total Voice Playout Duration for Active Voice by adding the OnTimeRvPlayout value to the GapFill values.
OutSignalLevel	Active output signal level to the telephony interface used by this call.
PeerAddress	Destination pattern or number associated with this peer.
PeerId	ID value of the peer table entry to which this call was made.
PeerIfIndex	Voice port index number for this peer. For ISDN media, this would be the index number of the B channel used for this call.
PeerSubAddress	Subaddress when this call is connected.
Percent Packet Loss	Total percent packet loss.
Port	Identification of the time-division multiplexing (TDM) voice port carrying the call.

Field	Description
ReceiveBytes	Number of bytes received by the peer during this call.
ReceiveDelay	Average Playout FIFO Delay plus the Decoder Delay during this voice call, in ms.
ReceivePackets	Number of packets received by this peer during this call.
ReleaseSource	Number value of the release source.
RemoteIPAddress	Remote system IP address for the VoIP call.
RemoteUDPPort	Remote system User Datagram Protocol (UDP) listener port to which voice packets are sent.
RoundTripDelay	Voice packet round-trip delay between the local and remote systems on the IP backbone for this call.
SelectedQoS	Selected Resourse Reservation Protocol (RSVP) quality of service (QoS) for this call.
SessionProtocol	Session protocol used for an Internet call between the local and remote routers through the IP backbone.
SessionTarget	Session target of the peer used for this call.
SetupTime	Value of the system UpTime, in milliseconds, when the call associated with this entry was started.
SignalingType	Signaling type for this call; for example, channel-associated signaling (CAS) or common channel signaling (CCS).
SIP call-legs	Total Session Initiation Protocol (SIP) call legs for which call records are available.
Telephony call-legs	Total telephony call legs for which call records are available.
Time between Buffer Drain/Fills	Minimum and maximum durations between jitter buffer drain or fill events, in seconds.
TransmitBytes	Number of bytes sent by this peer during this call.
TransmitPackets	Number of packets sent by this peer during this call.
TxDuration	The length of the call. Appears only if the medium is TELE.
VAD	Whether voice activation detection (VAD) was enabled for this call.
VoiceTxDuration	Duration of voice transmission from this peer to the voice gateway for this call, in ms. Derive the Voice Utilization Rate by dividing the VoiceTxDuration value by the TxDuration value.

The following is sample output from the **show call active fax brief** command:

```
Router# show call active fax brief
<ID>: <start>hs.<index> +<connect> pid:<peer_id> <dir> <addr> <state> \
  tx:<packets>/<bytes> rx:<packets>/<bytes> <state>
IP <ip>:<udp> rtt:<time>ms pl:<play>/<gap>ms lost:<lost>/<early>/<late>
  delay:<last>/<min>/<max>ms <codec>
FR <protocol> [int dlci cid] vad:<y/n> dtmf:<y/n> seq:<y/n>
  sig:<on/off> <codec> (payload size)
Tele <int>: tx:<tot>/<v>/<fax>ms <codec> noise:<l> acom:<l> i/o:<l>/<l> dBm

1    : 22021hs.1 +2263 pid:0 Answer wook song active
tx:0/0 rx:0/41190
IP 0.0.0.0 AcceptedMime:2 DiscardedMime:1

1    : 23193hs.1 +1091 pid:3469 Originate 527.... active
tx:10/13838 rx:0/0
Tele : tx:31200/10910/20290ms  noise:-1 acom:-1  i/0:0/0 dBm
```

The following is sample output from the **show call active fax** command displaying T.38 fax relay statistics:

```
Router# show call active fax
Telephony call-legs: 1
SIP call-legs: 0
H323 call-legs: 0
MGCP call-legs: 0
Multicast call-legs: 0
Total call-legs: 1
 GENERIC:
SetupTime=1874690 ms
Index=1
PeerAddress=5551234
PeerSubAddress=
PeerId=3
PeerIfIndex=244
LogicalIfIndex=118
ConnectTime=187875
CallDuration=00:00:44 sec
CallState=4
CallOrigin=2
ChargedUnits=0
InfoType=fax
TransmitPackets=309
TransmitBytes=5661
ReceivePackets=1124
ReceiveBytes=49189
TELE:
ConnectionId=[0x6B241E98 0xA78111D8 0x8002000A 0xF4107CA0]
IncomingConnectionId=[0x6B241E98 0xA78111D8 0x8002000A 0xF4107CA0]
CallID=1
Port=3/0/0 (1)
BearerChannel=3/0/0.1
TxDuration=2840 ms
VoiceTxDuration=0 ms
FaxTxDuration=0 ms
FaxRate=disable bps
FaxRelayMaxJitBufDepth 346
FaxRelayJitterBufOverflow 0
Initial HS Modulation is V.17/long/14400
Recent HS modulation is V.17/short/14400
Number of pages 1
Direction of transmission is Transmit
Num of Packets TX'ed/RX'ed 932/52
```

```
Packet loss conceal is 0
Encapsulation protocol is T.38 (UDPTL)
ECM is DISABLED
NoiseLevel=0
ACOMLevel=0
OutSignalLevel=0
InSignalLevel=0
InfoActivity=0
ERLLevel=0
SessionTarget=
ImgPages=0
CallerName=
CallerIDBlocked=False
OriginalCallingNumber=5551234
OriginalCallingOctet=0x80
OriginalCalledNumber=5555678
OriginalCalledOctet=0x80
OriginalRedirectCalledNumber=
OriginalRedirectCalledOctet=0xFF
TranslatedCallingNumber=5551234
TranslatedCallingOctet=0x80
TranslatedCalledNumber=5555678
TranslatedCalledOctet=0x80
TranslatedRedirectCalledNumber=
TranslatedRedirectCalledOctet=0xFF
GwReceivedCalledNumber=5555678
GwReceivedCalledOctet3=0x80
GwReceivedCallingNumber=5551234
GwReceivedCallingOctet3=0x80
GwReceivedCallingOctet3a=0x0
DSPIdentifier=1/0:0
Telephony call-legs: 1
SIP call-legs: 0
H323 call-legs: 0
MGCP call-legs: 0
Multicast call-legs: 0
Total call-legs: 1
```

The table below provides an alphabetical listing of the fields displayed in the output of the **show call active fax**command for T.38 fax relay statistics and a description of each field.

Table 14: show call active fax Field Descriptions for Significant T.38 Fax Relay Statistics

Field	Description
ACOMLevel	Current ACOM level estimate in 0.1 dB increments. The term ACOM is used in G.165, *General Characteristics of International Telephone Connections and International Telephone Circuits: Echo Cancellers* . ACOM is the combined loss achieved by the echo canceller, which is the sum of the ERL, ERL enhancement, and nonlinear processing loss for the call.
BearerChannel	Identification of the bearer channel carrying the call.
ERLLevel	Current ERL level estimate in 0.1 dB increments.
FaxRate	Fax transmission rate from this peer to the specified dial peer, in bits per second (bps).
FaxRelayJitterBufOverflow	Fax relay jitter buffer overflow, in ms.

Field	Description
FaxRelayMaxJitBufDepth	Fax relay maximum jitter buffer depth, in ms.
FaxTxDuration	Duration of fax transmission from this peer to the voice gateway for this call, in ms.
GwReceivedCalledNumber, GwReceivedCalledOctet3	Call information received at the gateway.
H323 call-legs	Type of call: H.323.
Initial HS Modulation	Initial high speed modulation used.
LogicalIfIndex	Index number of the logical interface for this call.
MGCP call-legs	Type of call: Media Gateway Control Protocol (MGCP).
Multicast call-legs	Type of call: Multicast.
OriginalCallingNumber, OriginalCalling Octet, OriginalCalledNumber, OriginalCalledOctet, OriginalRedirectCalledNumber, OriginalRedirectCalledOctet	Original call information regarding calling, called, and redirect numbers, and octet-3s. Octet-3s are information elements (IEs) of Q.931 that include type of number, numbering plan indicator, presentation indicator, and redirect reason information.
PeerIfIndex	Voice port index number for this peer. For ISDN media, this would be the index number of the B channel used for this call.
Port	Identification of the TDM voice port carrying the call.
Recent HS Modulation	Most recent high-speed modulation used.
SIP call-legs	Type of call: SIP.
Telephony call-legs	Type of call: Telephony.
Total call-legs	Total calls.
TranslatedCallingNumber, TranslatedCallingOctet, TranslatedCalledNumber, TranslatedCalledOctet, TranslatedRedirectCalledNumber, TranslatedRedirectCalledOctet	Translated call information.
TxDuration	Duration of transmit path open from this peer to the voice gateway for this call, in ms.
VoiceTxDuration	Duration of voice transmission from this peer to the voice gateway for this call, in ms.

Related Commands

Command	Description
show call active voice	Displays call information for voice calls that are in progress.
show call history	Displays the call history table.
show call-router routes	Displays the dynamic routes in the cache of the BE.
show call-router status	Displays the Annex G BE status.
show voice port	Displays configuration information about a specific voice port.

show call active media

To display call information for media calls in progress, use the **show call active media** command in user EXEC or privileged EXEC mode.

show call active media [[**brief**] [**id** *identifier*] | **compact** [**duration** {**less** *seconds* | **more** *seconds*}]]

Syntax Description

brief	(Optional) Displays a truncated version of call information.
id *identifier*	(Optional) Displays only the call with the specified *identifier*. The range is a hexadecimal value from 1 to FFFF.
compact	(Optional) Displays a compact version of call information.
duration	(Optional) Displays the call history for the specified time duration.
less *seconds*	(Optional) Displays the call history for shorter duration calls, in seconds. The range is from 1 to 2147483647.
more *seconds*	(Optional) Displays the call history for longer duration calls, in seconds. The range is from 1 to 2147483647.

Command Modes

User EXEC (>)
Privileged EXEC (#)

Command History

Release	Modification
12.4(15)T	This command was introduced.
12.4(18)M	This command was modified. The **less**keyword, **more**keyword, and *seconds* argument were added.

Usage Guidelines

Use this command to display the contents of the active call table. This command displays information about call times, dial peers, connections, quality of service, and other status and statistical information for media calls currently connected through the router.

When a media call is no longer active, its record is stored. You can display the record by using the **show call history media**command.

Examples

The following is sample output from the **show call active media**command:

```
Router# show call active media
Telephony call-legs: 0
SIP call-legs: 0
H323 call-legs: 0
Call agent controlled call-legs: 0
SCCP call-legs: 0
Multicast call-legs: 0
Media call-legs: 2
Total call-legs: 2
```

```
 GENERIC:
SetupTime=408040 ms
Index=1
PeerAddress=sip:mrcpv2TTSServer@10.5.18.224:5060
PeerSubAddress=
PeerId=2235
PeerIfIndex=185
LogicalIfIndex=0
ConnectTime=408130 ms
CallDuration=00:00:01 sec
CallState=4
CallOrigin=1
ChargedUnits=0
InfoType=speech
TransmitPackets=0
TransmitBytes=0
ReceivePackets=57
ReceiveBytes=9120
VOIP-MEDIA:
ConnectionId[0x6B02FC0C 0xC3511DB 0x8006000B 0x5FDA0EF4]
IncomingConnectionId[0x6B02FC0C 0xC3511DB 0x8006000B 0x5FDA0EF4]
CallID=18
RemoteIPAddress=10.5.18.224
RemoteUDPPort=10000
RemoteSignallingIPAddress=10.5.18.224
RemoteSignallingPort=5060
RemoteMediaIPAddress=10.5.18.224
RemoteMediaPort=10000
RoundTripDelay=0 ms
SelectedQoS=best-effort
tx_DtmfRelay=rtp-nte
FastConnect=FALSE
AnnexE=FALSE
Separate H245 Connection=FALSE
H245 Tunneling=FALSE
SessionProtocol=sipv2
ProtocolCallId=6B0CC055-C3511DB-801BC48C-6A894889@10.5.14.2
SessionTarget=10.5.18.224
OnTimeRvPlayout=0
GapFillWithSilence=0 ms
GapFillWithPrediction=0 ms
GapFillWithInterpolation=0 ms
GapFillWithRedundancy=0 ms
HiWaterPlayoutDelay=0 ms
LoWaterPlayoutDelay=0 ms
TxPakNumber=0
TxSignalPak=0
TxComfortNoisePak=0
TxDuration=0
TxVoiceDuration=0
RxPakNumber=0
RxSignalPak=0
RxComfortNoisePak=0
RxDuration=0
RxVoiceDuration=0
RxOutOfSeq=0
RxLatePak=0
RxEarlyPak=0
RxBadProtocol=0
PlayDelayCurrent=0
PlayDelayMin=0
PlayDelayMax=0
PlayDelayClockOffset=0
PlayDelayJitter=0
```

```
PlayErrPredictive=0
PlayErrInterpolative=0
PlayErrSilence=0
PlayErrBufferOverFlow=0
PlayErrRetroactive=0
PlayErrTalkspurt=0
OutSignalLevel=0
InSignalLevel=0
LevelTxPowerMean=0
LevelRxPowerMean=0
LevelBgNoise=0
ERLLevel=0
ACOMLevel=0
ErrRxDrop=0
ErrTxDrop=0
ErrTxControl=0
ErrRxControl=0
Source tg label=test5
ReceiveDelay=0 ms
LostPackets=0
EarlyPackets=0
LatePackets=0
SRTP = off
TextRelay = off
VAD = disabled
CoderTypeRate=g711ulaw
CodecBytes=160
Media Setting=flow-through
CallerName=
CallerIDBlocked=False
OriginalCallingNumber=
OriginalCallingOctet=0x0
OriginalCalledNumber=
OriginalCalledOctet=0x0
OriginalRedirectCalledNumber=
OriginalRedirectCalledOctet=0x0
TranslatedCallingNumber=4085254655
TranslatedCallingOctet=0x21
TranslatedCalledNumber=
TranslatedCalledOctet=0xC1
TranslatedRedirectCalledNumber=
TranslatedRedirectCalledOctet=0xFF
GwOutpulsedCallingNumber=4085254655
GwOutpulsedCallingOctet3=0x21
GwOutpulsedCallingOctet3a=0x81
MediaInactiveDetected=no
MediaInactiveTimestamp=
MediaControlReceived=
LongDurationCallDetected=no
LongDurCallTimestamp=
LongDurcallDuration=
Username=
 GENERIC:
SetupTime=408050 ms
Index=1
PeerAddress=sip:mrcpv2ASRServer@10.5.18.224:5060
PeerSubAddress=
PeerId=2234
PeerIfIndex=184
LogicalIfIndex=0
ConnectTime=408160 ms
CallDuration=00:00:03 sec
CallState=4
CallOrigin=1
```

```
ChargedUnits=0
InfoType=speech
TransmitPackets=188
TransmitBytes=30080
ReceivePackets=0
ReceiveBytes=0
VOIP-MEDIA:
ConnectionId[0x6B02FC0C 0xC3511DB 0x8006000B 0x5FDA0EF4]
IncomingConnectionId[0x6B02FC0C 0xC3511DB 0x8006000B 0x5FDA0EF4]
CallID=19
RemoteIPAddress=10.5.18.224
RemoteUDPPort=10002
RemoteSignallingIPAddress=10.5.18.224
RemoteSignallingPort=5060
RemoteMediaIPAddress=10.5.18.224
RemoteMediaPort=10002
RoundTripDelay=0 ms
SelectedQoS=best-effort
tx_DtmfRelay=rtp-nte
FastConnect=FALSE
AnnexE=FALSE
Separate H245 Connection=FALSE
H245 Tunneling=FALSE
SessionProtocol=sipv2
ProtocolCallId=6B0E94CD-C3511DB-801DC48C-6A894889@10.5.14.2
SessionTarget=10.5.18.224
OnTimeRvPlayout=1000
GapFillWithSilence=0 ms
GapFillWithPrediction=0 ms
GapFillWithInterpolation=1495 ms
GapFillWithRedundancy=0 ms
HiWaterPlayoutDelay=100 ms
LoWaterPlayoutDelay=95 ms
TxPakNumber=0
TxSignalPak=0
TxComfortNoisePak=0
TxDuration=0
TxVoiceDuration=0
RxPakNumber=0
RxSignalPak=0
RxComfortNoisePak=0
RxDuration=0
RxVoiceDuration=0
RxOutOfSeq=0
RxLatePak=0
RxEarlyPak=0
RxBadProtocol=0
PlayDelayCurrent=0
PlayDelayMin=0
PlayDelayMax=0
PlayDelayClockOffset=0
PlayDelayJitter=0
PlayErrPredictive=0
PlayErrInterpolative=0
PlayErrSilence=0
PlayErrBufferOverFlow=0
PlayErrRetroactive=0
PlayErrTalkspurt=0
OutSignalLevel=0
InSignalLevel=0
LevelTxPowerMean=0
LevelRxPowerMean=0
LevelBgNoise=0
ERLLevel=0
```

```
ACOMLevel=0
ErrRxDrop=0
ErrTxDrop=0
ErrTxControl=0
ErrRxControl=0
Source tg label=test5
ReceiveDelay=100 ms
LostPackets=0
EarlyPackets=0
LatePackets=0
SRTP = off
TextRelay = off
VAD = disabled
CoderTypeRate=g711ulaw
CodecBytes=160
Media Setting=flow-through
CallerName=
CallerIDBlocked=False
OriginalCallingNumber=
OriginalCallingOctet=0x0
OriginalCalledNumber=
OriginalCalledOctet=0x0
OriginalRedirectCalledNumber=
OriginalRedirectCalledOctet=0x0
TranslatedCallingNumber=4085254655
TranslatedCallingOctet=0x21
TranslatedCalledNumber=
TranslatedCalledOctet=0xC1
TranslatedRedirectCalledNumber=
TranslatedRedirectCalledOctet=0xFF
GwOutpulsedCallingNumber=4085254655
GwOutpulsedCallingOctet3=0x21
GwOutpulsedCallingOctet3a=0x81
MediaInactiveDetected=no
MediaInactiveTimestamp=
MediaControlReceived=
LongDurationCallDetected=no
LongDurCallTimestamp=
LongDurcallDuration=
Username=
Telephony call-legs: 0
SIP call-legs: 0
H323 call-legs: 0
Call agent controlled call-legs: 0
SCCP call-legs: 0
Multicast call-legs: 0
Media call-legs: 2
Total call-legs: 2
```

The table below describes the significant fields shown in the display.

Table 15: show call active media Field Descriptions

Field	Description
Telephony call-legs	Total telephony call legs for which call records are available.
SIP call-legs	Total session initiation protocol (SIP) call legs for which call records are available.
H323 call-legs	Total H.323 call legs for which call records are available.

Field	Description
Media	Medium over which the call is carried. If the call is carried over the (telephone) access side, the entry is TELE. If the call is carried over the voice network side, the entry is either ATM, FR (for Frame Relay), or HDLC (for High-Level Data Link Control).
GENERIC	Generic or common parameters, that is, parameters that are common for VoIP and telephony call legs.
SetupTime	Value of the system UpTime, in milliseconds, when the call associated with this entry was started.
Index	Dial peer identification number.
PeerAddress	Destination pattern or number associated with this peer.
PeerId	ID value of the peer table entry to which this call was made.
PeerIfIndex	Voice port index number for this peer. For ISDN media, this would be the index number of the B channel used for this call.
LogicalIfIndex	Index number of the logical interface for this call.
ConnectTime	Time, in milliseconds, at which the call was connected.
CallDuration	Length of the call, in hours, minutes, and seconds, hh:mm:ss.
CallOrigin	Call origin: answer or originate.
CallState	Current state of the call.
ChargedUnits	Total number of charging units that apply to this peer since system startup. The unit of measure for this field is hundredths of second.
InfoType	Information type for this call; for example, voice or fax.
TransmitBytes	Number of bytes sent by this peer during this call.
TransmitPackets	Number of packets sent by this peer during this call.
ReceivePackets	Number of packets received by this peer during this call.
ReceiveBytes	Number of bytes received by the peer during this call.
ReceiveDelay	Average Playout FIFO Delay plus the Decoder Delay during this voice call, in ms.
ConnectionId	Global call identifier for this gateway call.
RemoteIPAddress	Remote system IP address for the VoIP call.
RemoteUDPPort	Remote system User Datagram Protocol (UDP) listener port to which voice packets are sent.

Field	Description
SelectedQoS	Selected Resource Reservation Protocol (RSVP) quality of service (QoS) for this call.
SessionTarget	Session target of the peer used for this call.
OnTimeRvPlayout	Duration of voice playout from data received on time for this call. Derive the Total Voice Playout Duration for Active Voice by adding the OnTimeRvPlayout value to the GapFill values.
GapFillWithInterpolation	Duration of a voice signal played out with a signal synthesized from parameters, or samples of data preceding and following in time because voice data was lost or not received in time from the voice gateway for this call.
GapFillWithRedundancy	Duration of a voice signal played out with a signal synthesized from available redundancy parameters because voice data was lost or not received in time from the voice gateway for this call.
GapFillWithPrediction	Duration of the voice signal played out with signal synthesized from parameters, or samples of data preceding in time, because voice data was lost or not received in time from the voice gateway for this call. Examples of such pullout are frame-eraser and frame-concealment strategies in G.729 and G.723.1 compression algorithms.
GapFillWithSilence	Duration of a voice signal replaced with silence because voice data was lost or not received in time for this call.
HiWaterPlayoutDelay	High-water-mark Voice Playout FIFO Delay during this call, in ms.
LoWaterPlayoutDelay	Low-water-mark Voice Playout FIFO Delay during this call, in ms.
CodecBytes	Payload size, in bytes, for the codec used.
CoderTypeRate	Negotiated coder rate. This value specifies the send rate of voice or fax compression to its associated call leg for this call.
InSignalLevel	Active input signal level from the telephony interface used by this call.
OutSignalLevel	Active output signal level to the telephony interface used by this call.
ERLLevel	Current echo return loss (ERL) level for this call.
ACOMLevel	Current ACOM level for this call. ACOM is the combined loss achieved by the echo canceler, which is the sum of the Echo Return Loss, Echo Return Loss Enhancement, and nonlinear processing loss for the call.
PeerSubAddress	Subaddress when this call is connected.
RoundTripDelay	Voice packet round-trip delay between the local and remote systems on the IP backbone for this call.
SessionProtocol	Session protocol used for an Internet call between the local and remote routers through the IP backbone.

Field	Description
TxDuration	The length of the call. Appears only if the medium is TELE.
VAD	Whether voice activation detection (VAD) was enabled for this call.

Related Commands

Command	Description
show call history media	Displays the call history table.

show call active total-calls

To display the total number of calls in progress, use the **show call active total-calls** command in user EXEC or privileged EXEC mode.

show call active total-calls

Syntax Description

This command has no arguments or keywords.

Command Modes

User EXEC (>)

Privileged EXEC (#)

Command History

Release	Modification
15.3(3)M	This command was introduced.

Example

The following example shows how to view the total number of active calls:

```
Device# show call active total-calls
Total Number of Active Calls : 110
```

show call active video

To display call information for Signaling Connection Control Protocol (SCCP), Session Initiation Protocol (SIP), and H.323 video calls in progress, use the **show call active video** command in user EXEC or privileged EXEC mode.

show call active video [[**brief**] [**id** *call-identifier*] | **compact** [**duration** {**less** | **more**} *seconds*] | **echo-canceller** *call-id* | **session-id** *WORD* | **stats**]

Syntax Description

brief	(Optional) Displays a truncated version of active video call information.
id *call-identifier*	(Optional) Displays only the video calls with the specified identifier. The range is from 1 to FFFF.
compact	(Optional) Displays a compact version of active video call information.
duration	(Optional) Displays call history for the specified time duration.
less	Displays call history for shorter duration calls.
more	Displays call history for longer duration calls.
seconds	Time, in seconds. The range is from 1 to 2147483647.
echo-canceller *call-id*	(Optional) Displays information about the state of the extended echo canceller (EC). The range is from 0 to FFFFFFFF.
session-id *WORD*	(Optional) Displays session identifier details for a specific session-id. *WORD* specifies a wildcard pattern which is matched against the localUUID, RemoteUUID or complete Session-Id header string. A valid wildcard pattern can comprise one or more combination of any of these characters *, [0-9], [a-f], [A-F].
stats	(Optional) Displays information about DSP statistics and video quality metrics.

Command Modes

User EXEC (>)

Privileged EXEC (#)

Command History

Cisco IOS Release	Cisco Product	Modification
12.4(4)XC	Cisco Unified CME 4.0	This command was introduced.
12.4(9)T	Cisco Unified CME 4.0	This command was integrated into Cisco IOS Release 12.4(9)T.
12.4(11)T	--	This command was modified. Support was added for SIP and H.323 calls.

Cisco IOS Release	Cisco Product	Modification
12.4(16); 12.4(15)T	--	This command was modified. The Port and BearerChannel display fields were added to the TELE call leg record of the command output.
15.1(4)M	Cisco Unified CME 8.6	This command was modified. The **stats** keyword was added.
Cisco IOS 15.6(2)T Cisco IOS XE Denali 16.3.1	--	This command was modified. • The **session-id** keyword was added. • **show call active video brief** command output was enhanced to show VRF details and session-id details. • **show call active video compact** command output was enhanced to show VRF details.
Cisco IOS XE 17.16.1a	--	This command was modified to display SCIP video codec information. **Note** This feature is available in 'preview' mode as it includes limited functionality or incomplete software dependencies.

Usage Guidelines

Use the **show call active video** command to display the contents of the active video call table.

Before you can query the echo state, you need to know the hexadecimal ID. Use the **show call active video brief** command to find the hexadecimal ID.

Examples

The following is a sample compact output for SCIP video codec traffic:

```
 Router # show call active video compact
  <callID>  A/O FAX  T<sec>  Codec  type        Peer Address   IP R<ip>:<udp>     VRF
Total call-legs: 2
  11        ANS      T6      scip   VOIP-VIDEO   P1234         10.64.86.70:6011    NA

  13        ORG      T6      scip   VOIP-VIDEO   P1111         10.64.86.70:6007    NA
```

The following is a sample brief output for SCIP video codec traffic:

```
 Router # show call active video brief
Telephony call-legs: 0
SIP call-legs: 2
H323 call-legs: 0
Call agent controlled call-legs: 0
SCCP call-legs: 0
STCAPP call-legs: 0
Multicast call-legs: 0
Total call-legs: 2
1215 : 15 2673580ms.1 (*11:49:40.800 UTC Tue Jul 23 2024) +1010 pid:666 Answer 1234 active
 dur 00:00:27 tx:12/10266 rx:12/10266 dscp:0 media:0 audio tos:0xB8 video tos:0x88
 IP 10.64.86.70:6007 SRTP: off rtt:0ms pl:0/0ms lost:0/0/0 delay:0/0/0ms scip TextRelay:
off Transcoded: No ICE: Off
```

```
 media inactive detected:n media contrl rcvd:n/a timestamp:n/a
 long duration call detected:n long duration call duration:n/a timestamp:n/a
 LostPacketRate:0.00 OutOfOrderRate:0.00
 LocalUUID:a97cadb85d17540b97f11e5f891a4425
 RemoteUUID:8a790915375e57d59d825b012bc9d145
 VRF: NA
1215 : 17 2673580ms.2 (*11:49:40.800 UTC Tue Jul 23 2024) +1010 pid:777 Originate 1111
active
 dur 00:00:27 tx:12/10266 rx:12/10266 dscp:0 media:0 audio tos:0xB8 video tos:0x88
 IP 10.64.86.70:6003 SRTP: off rtt:0ms pl:0/0ms lost:0/0/0 delay:0/0/0ms scip TextRelay:
off Transcoded: No ICE: Off
 media inactive detected:n media contrl rcvd:n/a timestamp:n/a
 long duration call detected:n long duration call duration:n/a timestamp:n/a
 LostPacketRate:0.00 OutOfOrderRate:0.00
 LocalUUID:8a790915375e57d59d825b012bc9d145
 RemoteUUID:a97cadb85d17540b97f11e5f891a4425
 VRF: NA

Telephony call-legs: 0
SIP call-legs: 2
H323 call-legs: 0
Call agent controlled call-legs: 0
SCCP call-legs: 0
STCAPP call-legs: 0
Multicast call-legs: 0
Total call-legs: 2
```

The following is sample output from the **show call active video brief** command:

```
Router # show call active video brief
<ID>: <CallID> <start>ms.<index> (<start>) +<connect> pid:<peer_id> <dir> <addr> <state>
  dur hh:mm:ss tx:<packets>/<bytes> rx:<packets>/<bytes> dscp:<packets violation>
media:<packets violation> audio tos:<audio tos value> video tos:<video tos value>
 IP <ip>:<udp> rtt:<time>ms pl:<play>/<gap>ms lost:<lost>/<early>/<late>
  delay:<last>/<min>/<max>ms <codec> <textrelay> <transcoded

 media inactive detected:<y/n> media cntrl rcvd:<y/n> timestamp:<time>

 long duration call detected:<y/n> long duration call duration :<sec> timestamp:<time>
 LostPacketRate:<%> OutOfOrderRate:<%>
LocalUUID: <%> RemoteUUID: <%>
 VRF:<%>
  MODEMPASS <method> buf:<fills>/<drains> loss <overall%> <multipkt>/<corrected>
   last <buf event time>s dur:<Min>/<Max>s
 FR <protocol> [int dlci cid] vad:<y/n> dtmf:<y/n> seq:<y/n>
  <codec> (payload size)
 ATM <protocol> [int vpi/vci cid] vad:<y/n> dtmf:<y/n> seq:<y/n>
  <codec> (payload size)
 Tele <int> (callID) [channel_id] tx:<tot>/<v>/<fax>ms <codec> noise:<l> acom:<l> i/o:<l>/<l>
 dBm
  MODEMRELAY info:<rcvd>/<sent>/<resent> xid:<rcvd>/<sent> total:<rcvd>/<sent>/<drops>
         speeds(bps): local <rx>/<tx> remote <rx>/<tx>
 Proxy <ip>:<audio udp>,<video udp>,<tcp0>,<tcp1>,<tcp2>,<tcp3> endpt: <type>/<manf>
 bw: <req>/<act> codec: <audio>/<video>
  tx: <audio pkts>/<audio bytes>,<video pkts>/<video bytes>,<t120 pkts>/<t120 bytes>
 rx: <audio pkts>/<audio bytes>,<video pkts>/<video bytes>,<t120 pkts>/<t120 bytes>

Telephony call-legs: 0
SIP call-legs: 1
H323 call-legs: 0
Call agent controlled call-legs: 0
SCCP call-legs: 0
```

```
Multicast call-legs: 0
Total call-legs: 1
11EC : 2 798700ms.1 (*12:49:45.019 IST Tue Jan 12 2016) +2010 pid:441 Answer sipp connected

 dur 00:00:50 tx:0/0 rx:0/0 dscp:0 media:0 audio tos:0xB8 video tos:0x0
 IP 10.64.86.70:6005 SRTP: off rtt:0ms pl:0/0ms lost:0/0/0 delay:0/0/0ms g711ulaw TextRelay:
 off Transcoded: No ICE: Off
 media inactive detected:n media contrl rcvd:n/a timestamp:n/a
 long duration call detected:n long duration call duration:n/a timestamp:n/a
 LostPacketRate:0.00 OutOfOrderRate:0.00
LocalUUID : ab30317f1a784dc48ff824d0d3715d86
RemoteUUID : 47755a9de7794ba387653f2099600ef2
 VRF: VRF1

Telephony call-legs: 0
SIP call-legs: 1
H323 call-legs: 0
Call agent controlled call-legs: 0
SCCP call-legs: 0
Multicast call-legs: 0
Total call-legs: 1
```

The following is sample output from the **show call active video** command:

```
Router# show call active video
Telephony call-legs: 4
SIP call-legs: 0
H323 call-legs: 0
Call agent controlled call-legs: 0
SCCP call-legs: 2
Multicast call-legs: 0
Total call-legs: 6
 GENERIC:
SetupTime=169281770 ms
Index=2
PeerAddress=
PeerSubAddress=
PeerId=0
PeerIfIndex=0
LogicalIfIndex=0
ConnectTime=169281770 ms
CallDuration=01:20:44 sec
CallState=2
CallOrigin=1
ChargedUnits=0
InfoType=speech
TransmitPackets=819728
TransmitBytes=571031017
ReceivePackets=796308
ReceiveBytes=566120602
VOIP:
ConnectionId[0x0 0x0 0x0 0x0]
IncomingConnectionId[0x0 0x0 0x0 0x0]
CallID=85
GlobalCallId=[0x0 0x0 0x0 0x0]
CallReferenceId=25666520
CallServiceType=Video Conference
RTP Loopback Call=FALSE
sessionIDLocaluuid=6f0a93a3a79451aebeb6d83f79a3359f
sessionIDRemoteuuid=a55b0f45861551b88f57d1fb5bb23f89
RemoteIPAddress=0.0.0.0 RemoteUDPPort=2000
RemoteSignallingIPAddress=0.0.0.0
RemoteSignallingPort=0
RemoteMediaIPAddress=1.4.211.39
```

```
RemoteMediaPort=2000
RoundTripDelay=0 ms
SelectedQoS=best-effort
tx_DtmfRelay=inband-voice
FastConnect=FALSE
AnnexE=FALSE
Separate H245 Connection=FALSE
H245 Tunneling=FALSE
SessionProtocol=other
ProtocolCallId= sipv2
SessionTarget= 1.4.211.39
SafEnabled=FALSE
OnTimeRvPlayout=0
GapFillWithSilence=0 ms
GapFillWithPrediction=0 ms
GapFillWithInterpolation=0 ms
GapFillWithRedundancy=0 ms
HiWaterPlayoutDelay=0ms
LoWaterPlayoutDelay=0 ms
Video Conferee Statistics ConfereeActualFrameRate=0
ConfereeActualBitrate=934600
ConfereeTotalRxPackets=129853
ConfereeTotalRxBytes=125825024
ConfereeTotalTxPackets=129853
ConfereeTotalTxBytes=125825085
ConfereeTotalPacketsDropped=313
ConfereeCurrentPacketsDropped=0
ConfereeTotalPacketsOutOfOrder=296
ConfereeCurrentPacketsOutOfOrder=0
ConfereeMaxJitter=0 ConfereeCurJitter=0
ConfereeMaxDelay=0
ConfereeCurDelay=0
ConfereeMaxOutOfSyncDelay=0
ConfereeCurrentOutOfSyncDelay=0
ConfereeFastVideoUpdateRate=0
ConfereeVideoDuration=1076
Video Quality Scores RxVideoMOSInstant=78/100 (Good)
RxVideoMOSAverage=70/100 (Good)
VIDEO: VideoTransmitCodec=H264
VideoTransmitPictureWidth=640
VideoTransmitPictureHeight=480
VideoTransmitFrameRate=30
VideoTransmitBitrate=934600 bps
VideoTransmitLevel=2
VideoTransmitProfile=Baseline
VideoTransmitPayloadFormat=RFC3984
VideoTransmitPackets=129853
VideoTransmitBytes=125825085
VideoTransmitDuration=1076 seconds
VideoReceiveCodec=H264
VideoReceivePictureWidth=640
VideoReceivePictureHeight=480
VideoReceiveFrameRate=30
VideoReceiveBitrate=934600 bps
VideoReceiveLevel=2
VideoReceiveProfile=Baseline
VideoReceivePayloadFormat=RFC3984
VideoReceivePackets=129853
VideoReceiveBytes=125825024
VideoReceiveDuration=1076 seconds
VideoCap_Codec=H264
VideoCap_Format=CUSTOM
VideoCap_PictureWidth=640
VideoCap_PictureHeight=480
```

```
VideoCap_FrameRate=30
VideoCap_Bitrate=960000 bps
VideoCap_Level=2
VideoCap_Profile=Baseline
VideoCap_PayloadFormat=RFC3984
VideoLostPackets=0
VideoEarlyPackets=0
VideoLatePackets=0
VideoUsedBandwidth=934600
VideoNumberOfChannels=0
PlayoutMode = undefined
PlayoutInitialDelay=0 ms
ReceiveDelay=0 ms
LostPackets=0
EarlyPackets=0
LatePackets=0
SRTP = off
TextRelay = off
VAD =disabled
CoderTypeRate=h264
CodecBytes=0
Media Setting=flow-around
CallerName=
CallerIDBlocked=False
OriginalCallingNumber=
OriginalCallingOctet=0x0
OriginalCalledNumber=
OriginalCalledOctet=0x0
OriginalRedirectCalledNumber=
OriginalRedirectCalledOctet=0x0
TranslatedCallingNumber=
TranslatedCallingOctet=0x0
TranslatedCalledNumber=
TranslatedCalledOctet=0x0
TranslatedRedirectCalledNumber=
TranslatedRedirectCalledOctet=0x0
MediaInactiveDetected=no
MediaInactiveTimestamp=
MediaControlReceived=
LongDurationCallDetected=no
LongDurCallTimestamp=
LongDurcallDuration=
Username= MlppServiceDomainNW=0 (none)
MlppServiceDomainID=
PrecedenceLevel=0
(PRECEDENCE_LEVEL_NONE)
```

The following shows sample output from the **show call active video stats** command:

```
Router# show call active video stats
<ID>: <CallID> <start>ms.<index> +<connect> +<disc> pid:<peer_id> <direction> <addr>
  dur hh:mm:ss tx:<packets>/<bytes> rx:<packets>/<bytes>
Telephony call-legs: 0
SIP call-legs: 0
H323 call-legs: 0
Call agent controlled call-legs: 0
SCCP call-legs: 1
Multicast call-legs: 0
Total call-legs: 1
0    : 5 *10:54:50.661 PDT Tue Jan 11 2011.2 +0 pid:0 Originate  connecting
 dur 00:17:27 tx:126342/122451295 rx:126640/122453063
Video Conferee Statistics
ConfereeActualFrameRate=0  ConfereeActualBitrate=934300
```

```
ConfereeTotalRxPackets=126166  ConfereeTotalRxBytes=122282402
ConfereeTotalTxPackets=126166  ConfereeTotalTxBytes=122282463
ConfereeTotalPacketsDropped=295  ConfereeCurrentPacketsDropped=0
ConfereeTotalPacketsOutOfOrder=278  ConfereeCurrentPacketsOutOfOrder=0
ConfereeMaxJitter=0  ConfereeCurJitter=0
ConfereeMaxDelay=0  ConfereeCurDelay=0
ConfereeMaxOutOfSyncDelay=0  ConfereeCurrentOutOfSyncDelay=0
ConfereeFastVideoUpdateRate=0  ConfereeVideoDuration=1046
Video Quality Scores
RxVideoMOSInstant=78/100 (Good)
  (Compression Degradation: 86%, Network Degradation: 13%, Transcoding Degradation: 0%)
RxVideoMOSAverage=70/100 (Good)
  (Compression Degradation: 93%, Network Degradation: 6%, Transcoding Degradation: 0%)
```

The following is sample output from the **show call active video** command using the **compact** keyword:

```
Router# show call active video compact
<callID>  A/O  FAX T<sec>   Codec   type     Peer    Address IP R<ip>:<udp>  VRF
Total call-legs: 2
10193925 ANS   T22          H.264 VOIP-VIDEO P2005    10.0.0.1:18070         VRF1
10193927 ORG   T22          H.264 VOIP-VIDEO P3001    11.0.0.1:27008         VRF2
```

The table below describes the significant fields shown in the display, in alphabetical order.

Table 16: show call active video Field Descriptions

Field	Description
CallDuration	Length of the call, in hours, minutes, and seconds, hh:mm:ss.
CallState	Current state of the call.
Call agent controlled call-legs	Displays call legs for devices that are not telephony endpoints; for example, transcoding and conferencing
ChargedUnits	Total number of charging units that apply to this peer since system startup. The unit of measure for this field is hundredths of a second.
CodecBytes	Payload size, in bytes, for the codec used.
CoderTypeRate	Negotiated coder rate. This value specifies the send rate of voice or fax compression to its associated call leg for this call.
ConnectionId	Global call identifier for this gateway call.
ConnectTime	Time, in milliseconds (ms), during which the call was connected.
EchoCancellerMaxReflector	Size of the largest reflector, in ms. The reflector size cannot exceed the configured echo path capacity. For example, if 32 ms is configured, the reflector does not report capacity beyond 32 ms.
ERLLevel	Current echo return loss (ERL) level for this call.
FaxTxDuration	Duration, in ms, of fax transmission from this peer to the voice gateway for this call. You can derive the Fax Utilization Rate by dividing the FaxTxDuration value by the TxDuration value.

Field	Description
GapFillWithInterpolation	Duration, in ms, of a voice signal played out with a signal synthesized from parameters, or samples of data preceding and following in time because voice data was lost or not received in time from the voice gateway for this call.
GapFillWithRedundancy	Duration, in ms, of a voice signal played out with a signal synthesized from available redundancy parameters because voice data was lost or not received in time from the voice gateway for this call.
GapFillWithPrediction	Duration, in ms, of the voice signal played out with a signal synthesized from parameters, or samples of data preceding in time, because voice data was lost or not received in time from the voice gateway for this call. Examples of such pullout are frame-eraser and frame-concealment strategies in G.729 and G.723.1 compression algorithms.
GapFillWithSilence	Duration, in ms, of a voice signal replaced with silence because voice data was lost or not received in time for this call.
GENERIC	Generic or common parameters, that is, parameters that are common for VoIP and telephony call legs.
H320CallType	Total H320 call types available.
H323 call-legs	Total H.323 call legs for which call records are available.
HiWaterPlayoutDelay	High-water-mark voice playout first in first out (FIFO) delay during this call, in ms.
Index	Dial peer identification number.
InfoActivity	Active information transfer activity state for this call.
InfoType	Information type for this call; for example, voice, speech, or fax.
InSignalLevel	Active input signal level from the telephony interface used by this call.
Last Buffer Drain/Fill Event	Elapsed time since the last jitter buffer drain or fill event, in seconds.
LocalHostname	Local hostnames used for locally generated gateway URLs.
LogicalIfIndex	Index number of the logical interface for this call.
LoWaterPlayoutDelay	Low-water-mark voice playout FIFO delay during this call, in ms.
LowerIFName	Physical lower interface information. Appears only if the medium is ATM, Frame Relay (FR), or High-Level Data Link Control (HDLC).
Media	Medium over which the call is carried. If the call is carried over the (telephone) access side, the entry is TELE. If the call is carried over the voice network side, the entry is either ATM, FR, or HDLC.
Multicast call-legs	Total multicast call legs for which call records are available.
NoiseLevel	Active noise level for this call.

Field	Description
OnTimeRvPlayout	Duration of voice playout from data received on time for this call. Derive the Total Voice Playout Duration for Active Voice by adding the OnTimeRvPlayout value to the GapFill values.
OutSignalLevel	Active output signal level to the telephony interface used by this call.
PeerAddress	Destination pattern or number associated with this peer.
PeerId	ID value of the peer table entry to which this call was made.
PeerIfIndex	Voice port index number for this peer. For ISDN media, this would be the index number of the B channel used for this call.
PeerSubAddress	Subaddress when this call is connected.
ReceiveBytes	Number of bytes received by the peer during this call.
ReceiveDelay	Average playout FIFO delay plus the decoder delay during this voice call, in ms.
ReceivePackets	Number of packets received by this peer during this call.
RemoteIPAddress	Remote system IP address for the VoIP call.
RemoteUDPPort	Remote system User Datagram Protocol (UDP) listener port to which voice packets are sent.
RoundTripDelay	Voice packet round-trip delay, in ms, between the local and remote systems on the IP backbone for this call.
SCCP call-legs	Call legs for SCCP telephony endpoints.
SelectedQoS	Selected Resource Reservation Protocol (RSVP) quality of service (QoS) for this call.
SessionIDLocaluuid	UUID generated from originating user agent.
SessionIDRemoteuuid	UUID generated from terminating user agent.
SessionProtocol	Session protocol used for an Internet call between the local and remote routers through the IP backbone.
SessionTarget	Session target of the peer used for this call.
SetupTime	Value of the system UpTime, in milliseconds, when the call associated with this entry was started.
SIP call-legs	Total SIP call legs for which call records are available.
Telephony call-legs	Total telephony call legs for which call records are available.
Total call-legs	Total number of call legs for the call.
TransmitBytes	Number of bytes sent by this peer during this call.

Field	Description
TransmitPackets	Number of packets sent by this peer during this call.
TxDuration	The length of the call. Appears only if the medium is TELE.
VAD	Whether voice activation detection (VAD) was enabled for this call.
VideoCap_Annex	Extension of the video stream; for example, annex D1 and E.
VideoCap_Bitrate	Negotiated bitrate of the video stream; for example, 128000 b/s.
VideoCap_Codec	Codec for the active video call.
VideoCap_Format	Video format for the active video call.
VideoCap_FrameRate	Negotiated frame rate of the video stream; for example, 15 or 30 f/s.
VideoCap_PictureHeight	Height of the video resolution.
VideoCap_PictureWidth	Width of the video resolution.
VideoEarlyPackets	Number of early packets for a video call.
VideoLatePackets	Number of late packets in a video call.
VideoLostPackets	Number of lost packets in a video call.
VideoNumberOfChannels	Number of channels used for a video call.
Video Quality Score	Instantaneous and average Mean Opinion Score (MOS) for each active call leg. The MOS score is based on the amount of video quality degradation caused by compression distortion and the amount of video quality degradation caused by packet loss. The scale for the MOS score is as follows: • Excellent--(80--100) • Good--(60--80) • Fair--(40--60) • Poor--(20--40) • Bad--(0--20)
VideoReceiveBytes	Number of bytes received in the video call.
VideoReceiveCodec	Type of video codec used in the receiving stream.
VideoReceivePackets	Number of packets received in the video call.
VideoTransmitBytes	Number of bytes transmitted in the video call.
VideoTransmitCodec	Type of video codec used in the transmission stream.
VideoTransmitPackets	Number of packets transmitted in the video call.

Field	Description
VideoUsedBandwidth	Bandwidth, in kbps, used for a video call.
VoiceTxDuration	Duration of voice transmission from this peer to the voice gateway for this call, in milliseconds. Derive the Voice Utilization Rate by dividing the VoiceTxDuration value by the TxDuration value.

Related Commands

Command	Description
show call history video	Displays call history information for SCCP video calls.

show call active voice

To display call information for voice calls in progress, use the **show call active voice** command in user EXEC or privileged EXEC mode.

show call active voice [[**brief**] [**long-dur-call-inactive** | **media-inactive**] [**called-number** *number* | **calling-number** *number*] [**id** *call-identifier*] | **compact** [**duration** {**less** | **more**} *seconds*] | **dest-route-string** *tag* | **echo-canceller** {*hexadecimal-id* | **port** *slot-number* | **summary**} | **long-dur-call** [**called-number** *number* | **calling-number** *number*] | **redirect tbct** | **session-id** *word* | **stats**]

Syntax in Cisco IOS Release 12.2(33)SXH and Subsequent 12.2SX Releases
show call active [**brief**]

Syntax Description

brief	(Optional) Displays a truncated version of call information.
long-dur-call-inactive	(Optional) Displays long duration calls that are detected and notified.
media-inactive	(Optional) Displays information about inactive media that have been detected.
called-number *number*	(Optional) Displays a specific called number pattern.
calling-number *number*	(Optional) Displays a specific calling number pattern.
id *call-identifier*	(Optional) Displays only the call with the specified *call-identifier* value. The range is from 1 to FFFF.
compact	(Optional) Displays a compact version of call information.
duration	(Optional) Displays the call history for the specified time duration.
less *seconds*	Displays the call history for shorter duration calls, in seconds. The range is from 1 to 2147483647.
more *seconds*	Displays the call history for longer duration calls, in seconds. The range is from 1 to 2147483647.
dest-route-string *tag*	(Optional) Displays only the call with the specified destination route *tag* value. The range is from 1 to 10000.
echo-canceller	(Optional) Displays information about the state of the extended echo canceller (EC).
hexadecimal-id	The hexadecimal ID of an active voice call. The range is from 0x0 to 0xFFFFFFFF.
port *slot-number*	Displays EC details for a specified active voice port. The range varies depending on the voice ports available on the router.
summary	Displays an EC summary for all active voice calls.
long-dur-call	(Optional) Displays long duration calls that are detected and notified.

redirect	(Optional) Displays information about active calls that are being redirected using Release-to-Pivot (RTPvt) or Two B-Channel Transfer (TBCT).
tbct	Displays information about TBCT calls.
session-id *WORD*	(Optional) Displays session identifier details for a specific session-id. *WORD* specifies a wildcard pattern which is matched against the localUUID, RemoteUUID or complete Session-Id header string. A valid wildcard pattern can comprise one or more combination of any of these characters *, [0-9], [a-f], [A-F].
stats	(Optional) Displays information about digital signal processing (DSP) voice quality metrics.

Command Modes

User EXEC (>)

Privileged EXEC (#)

Command History

Release	Modification
11.3(1)T	This command was introduced.
12.0(3)XG	This command was modified. Support for Voice over Frame Relay (VoFR) was added.
12.0(4)XJ	This command was implemented for store-and-forward fax on the Cisco AS5300.
12.0(4)T	This command was implemented on the Cisco 7200 series.
12.0(7)XK	This command was implemented on the Cisco MC3810.
12.1(3)T	This command was implemented for modem pass-through over VoIP on the Cisco AS5300.
12.1(5)XM	This command was implemented on the Cisco AS5800.
12.1(5)XM2	The command was implemented on the Cisco AS5350 and Cisco AS5400.
12.2(2)XB1	This command was implemented on the Cisco AS5850.
12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T. Support was not included for the Cisco AS5300, Cisco AS5350, Cisco AS5400, and Cisco AS5850.
12.2(11)T	Support was added for the Cisco AS5300, Cisco AS5350, Cisco AS5400, and Cisco AS5850.
12.2(13)T	This command was modified. The **echo-canceller**keyword was added. The command output was modified with an extra reflector location when the extended EC is present; the largest reflector location is shown.
12.3(1)	This command was modified. The **redirect** keyword was added.

Release	Modification
12.3(4)T	This command was modified. The **called-number**, **calling-number**, and **media-inactive**keywords were added.
12.3(14)T	This command was modified. New output relating to Skinny Client Control Protocol (SCCP), SCCP Telephony Control Application (STCAPP), and modem pass-through traffic was added.
12.4(2)T	This command was modified. The LocalHostname display field was added to the VoIP call leg record and command output was enhanced to display modem relay physical layer and error correction protocols.
12.4(4)T	This command was modified. The **long-dur-call** keyword was added.
12.4(11)XW	This command was modified. The **stats** keyword was added.
12.4(15)T	This command was modified. The Port and BearerChannel display fields were added to the TELE call leg record of the command output.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
12.4(16)	This command was modified. The Port and BearerChannel display fields were added to the TELE call leg record of the command output.
12.4(22)T	This command was modified. Command output was updated to show IPv6 information.
15.3(3)M	This command was modified. The **dest-route-string** keyword was added.
Cisco IOS XE Release 3.10S	This command was integrated into Cisco IOS XE Release 3.10S.
Cisco IOS 15.6(2)T Cisco IOS XE Denali 16.3.1	This command was modified. • The **session-id** keyword was added. • **show call active voice brief** command output was enhanced to show VRF details and session-id details. • **show call active voice compact** command output was enhanced to show VRF details.
Cisco IOS XE 17.16.1a	This command was modified to display SCIP audio codec information. **Note** This feature is available in 'preview' mode as it includes limited functionality or incomplete software dependencies.

Usage Guidelines

Use this command to display the contents of the active voice call table. This command displays information about call times, dial peers, connections, and quality of service, and other status and statistical information for voice calls currently connected through the router.

Before you can query the echo state, you need to know the hexadecimal ID. To find the hexadecimal ID, enter the **show call active voice brief** command or use the **show voice call status** command.

When the extended EC is present, the **show call active voice** command displays the contents of the Ditech EC_CHAN_CTRL structure. The table below contains names and descriptions of the fields in the EC_CHAN_CTRL structure. The table also provides a listing of the information types associated with this command.

Use the **show call active voice dest-route-string** command to display only the active voice calls with call routing configured using specified destination-route-string globally and in dial-peer level.

Table 17: EC_CHAN_CTRL Field Descriptions

Symbol	Field	Description
BYP0	Channel bypass	• 1 = Transparent bypass; EC is disabled. • 0 = Cancel; EC is enabled.
TAIL3	Max tail	• 0 = 24 milliseconds. • 1 = 32 milliseconds. • 2 = 48 milliseconds. • 3 = 64 milliseconds. **Note** This field should be set just greater than the anticipated worst round-trip tail delay.
REC3	Residual echo control	• 0 = Cancel only; echo is the result of linear processing; no nonlinear processing is applied. • 1 = Suppress residual; residual echo is zeroed; simple nonlinear processing is applied (you might experience "dead air" when talking). • 2 = Reserved. • 3 = Generate comfort noise (default).
FRZ0	h-register hold	1 = Freezes h-register; used for testing.
HZ0	h-register clear	Sending the channel command with this bit set clears the h-register.
TD3	Modem tone disable	• 0 = Ignore 2100 Hz modem answer tone. • 1 = G.164 mode (bypass canceller if 2100 Hz tone). • 2 = R. • 3 = G.165 mode (bypass canceller for phase reversing tone only).

Symbol	Field	Description
ERL0	Echo return loss	• 0 = 6 decibel (dB). • 1 = 3 dB. • 2 = 0 dB. • 3 = R. Worst echo return loss (ERL) situation in which canceller still works.
HLC1	High level compensation	• 0 = No attenuation. • 1 = 6 dB if clipped. On loud circuits, the received direction can be attenuated 6 dB if clipping is observed.
R0	Reserved	Must be set to 0 to ensure compatibility with future releases.

Use the **show call active voice redirect tbct** command to monitor any active calls that implement RTPvt or TBCT.

When a call is no longer active, its record is stored. You can display the record by using the **show call history voice** command.

Examples

The following is a sample compact output for SCIP audio codec traffic:

```
 Router # show call active voice compact
 <callID>  A/O FAX  T<sec>  Codec  type  Peer Address  IP R<ip>:<udp>    VRF
Total call-legs: 2
  350      ANS      T6      scip   VOIP   Psipp        10.43.33.45:6006   NA

  351      ORG      T6      scip   VOIP   P8888        10.43.33.45:6002   NA
```

The following is a sample brief output for SCIP audio codec traffic:

```
 Router # show call active voice brief
Telephony call-legs: 0
SIP call-legs: 2
H323 call-legs: 0
Call agent controlled call-legs: 0
SCCP call-legs: 0
STCAPP call-legs: 0
Multicast call-legs: 0
Total call-legs: 2

121C : 19 2737820ms.1 (*11:50:45.045 UTC Tue Jul 23 2024) +1010 pid:666 Answer 1234 active
 dur 00:00:12 tx:0/0 rx:0/0 dscp:0 media:0 audio tos:0xB8 video tos:0x0
 IP 10.64.86.70:6008 SRTP: off rtt:0ms pl:0/0ms lost:0/0/0 delay:0/0/0ms scip TextRelay:
off Transcoded: No ICE: Off
 media inactive detected:n media contrl rcvd:n/a timestamp:n/a
 long duration call detected:n long duration call duration:n/a timestamp:n/a
 LostPacketRate:0.00 OutOfOrderRate:0.00
 LocalUUID:37110991b54051679f675479a6e93de7
 RemoteUUID:e74b1bf0678e5209915c03a9660cb00f
 VRF: NA
121C : 20 2737820ms.2 (*11:50:45.045 UTC Tue Jul 23 2024) +1010 pid:777 Originate 1111
```

```
active
 dur 00:00:12 tx:0/0 rx:0/0 dscp:0 media:0 audio tos:0xB8 video tos:0x0
 IP 10.64.86.70:6004 SRTP: off rtt:0ms pl:0/0ms lost:0/0/0 delay:0/0/0ms scip TextRelay:
off Transcoded: No ICE: Off
 media inactive detected:n media contrl rcvd:n/a timestamp:n/a
 long duration call detected:n long duration call duration:n/a timestamp:n/a
 LostPacketRate:0.00 OutOfOrderRate:0.00
 LocalUUID:e74b1bf0678e5209915c03a9660cb00f
 RemoteUUID:37110991b54051679f675479a6e93de7
 VRF: NA

Telephony call-legs: 0
SIP call-legs: 2
H323 call-legs: 0
Call agent controlled call-legs: 0
SCCP call-legs: 0
STCAPP call-legs: 0
Multicast call-legs: 0
Total call-legs: 2
```

The following is sample output from the **show call active voice** command for modem relay traffic:

```
Router# show call active voice
Modem Relay Local Rx Speed=0 bps
Modem Relay Local Tx Speed=0 bps
Modem Relay Remote Rx Speed=0 bps
Modem Relay Remote Tx Speed=0 bps
Modem Relay Phy Layer Protocol=v34
Modem Relay Ec Layer Protocol=v14
SPRTInfoFramesReceived=0
SPRTInfoTFramesSent=0
SPRTInfoTFramesResent=0
SPRTXidFramesReceived=0
SPRTXidFramesSent=0
SPRTTotalInfoBytesReceived=0
SPRTTotalInfoBytesSent=0
SPRTPacketDrops=0
```

The table below describes the significant fields shown in the display.

Table 18: show show call active voice Field Descriptions

Field	Description
Modem Relay Local Rx Speed	Download speed, in bits per second, of the local modem relay.
Modem Relay Local Tx Speed	Upload speed of the local modem relay.
Modem Relay Remote Rx Speed	Download speed of the remote modem relay.
Modem Relay Remote Tx Speed	Upload speed of the remote modem relay.
Modem Relay Phy Layer Protocol	Physical protocol of the modem relay.
Modem Relay Ec Layer Protocol	EC layer protocol of the modem relay.
SPRTInfoFramesReceived	Total number of simple packet relay transport (SPRT) protocol frames received.

Field	Description
SPRTInfoTFramesSent	Total number of SPRT frames sent.
SPRTInfoTFramesResent	Total number of SPRT frames sent again.
SPRTXidFramesReceived	Total number of SPRTS ID frames received.
SPRTXidFramesSent	Total number of SPRTS ID frames sent.
SPRTTotalInfoBytesReceived	Total number of SPRT bytes received.
SPRTTotalInfoBytesSent	Total number of SPRT bytes sent.
SPRTPacketDrops	Total number of SPRT packets dropped.

The following is sample output from the **show call active voice** command:

```
Router# show call active voice
Telephony call-legs: 1
SIP call-legs: 0
H323 call-legs: 1
Call agent controlled call-legs: 0
SCCP call-legs: 0
Multicast call-legs: 0
Total call-legs: 2
 GENERIC:
SetupTime=1072620 ms
Index=1
PeerAddress=9193927582
PeerSubAddress=
PeerId=8
PeerIfIndex=19
LogicalIfIndex=0
ConnectTime=1078940 ms
CallDuration=00:00:51 sec
CallState=4
CallOrigin=2
ChargedUnits=0
InfoType=speech
TransmitPackets=1490
TransmitBytes=0
ReceivePackets=2839
ReceiveBytes=56780
VOIP:
ConnectionId[0xE28B6D1D 0x3D9011D6 0x800400D0 0xBA0D97A1]
IncomingConnectionId[0xE28B6D1D 0x3D9011D6 0x800400D0 0xBA0D97A1]
CallID=1
sessionIDLocaluuid=4fd24d9121935531a7f8d750ad16e19
sessionIDRemoteuuid=db248b6cbdc547bbc6c6fdfb6916eeb
RemoteIPAddress=10.44.44.44 RemoteUDPPort=17096
RemoteSignallingIPAddress=10.44.44.44
RemoteSignallingPort=56434
RemoteMediaIPAddress=10.44.44.44
RemoteMediaPort=17096
RoundTripDelay=6 ms
SelectedQoS=best-effort
tx_DtmfRelay=h245-signal
FastConnect=TRUE AnnexE=FALSE
Separate H245 Connection=FALSE
H245 Tunneling=TRUE SessionProtocol=cisco
```

```
ProtocolCallId= sipv2
SessionTarget= 10.44.44.44
OnTimeRvPlayout=54160
GapFillWithSilence=0 ms
GapFillWithPrediction=0 ms
GapFillWithInterpolation=0 ms
GapFillWithRedundancy=0 ms
HiWaterPlayoutDelay=70 ms
LoWaterPlayoutDelay=60 ms
TxPakNumber=1490
TxSignalPak=0
TxComfortNoisePak=1
TxDuration=54240
TxVoiceDuration=29790
RxPakNumber=2711
RxSignalPak=0
RxDuration=0
TxVoiceDuration=54210
VoiceRxDuration=54160
RxOutOfSeq=0
RxLatePak=0
RxEarlyPak=0
PlayDelayCurrent=60
PlayDelayMin=60
PlayDelayMax=70
PlayDelayClockOffset=212491899
PlayDelayJitter=0 ms
PlayErrPredictive=0
PlayErrInterpolative=0
PlayErrSilence=0
PlayErrBufferOverFlow=10
PlayErrRetroactive=0
PlayErrTalkspurt=0
OutSignalLevel=-57
InSignalLevel=-51
LevelTxPowerMean=0
LevelRxPowerMean=-510
LevelBgNoise=0
ERLLevel=16
ACOMLevel=16
ErrRxDrop=0
ErrTxDrop=0
ErrTxControl=0
ErrRxControl=0
ReceiveDelay=60 ms
LostPackets=0
EarlyPackets=0
LatePackets=0
SRTP = off
VAD =enabled
CoderTypeRate=g729r8
CodecBytes=20
Media Setting=flow-through
CallerName=
CallerIDBlocked=False
OriginalCallingNumber=9193927582
OriginalCallingOctet=0x21
OriginalCalledNumber=93615494
OriginalCalledOctet=0xC1
OriginalRedirectCalledNumber=
OriginalRedirectCalledOctet=0xFF
TranslatedCallingNumber=9193927582
TranslatedCallingOctet=0x21
TranslatedCalledNumber=93615494
```

```
TranslatedCalledOctet=0xC1
TranslatedRedirectCalledNumber=
TranslatedRedirectCalledOctet=0xFF
GwReceivedCalledNumber=93615494
GwReceivedCalledOctet3=0xC1
GwReceivedCallingNumber=9193927582
GwReceivedCallingOctet3=0x21
GwReceivedCallingOctet3a=0x81
MediaInactiveDetected=no
MediaInactiveTimestamp=
MediaControlReceived=
Username= GENERIC:
SetupTime=1072760 ms
Index=1 PeerAddress=93615494
PeerSubAddress=
PeerId=9
PeerIfIndex=18
LogicalIfIndex=4
ConnectTime=1078940 ms
CallDuration=00:00:53 sec
CallState=4
CallOrigin=1
ChargedUnits=0
InfoType=speech
TransmitPackets=2953
TransmitBytes=82684
ReceivePackets=1490
ReceiveBytes=29781 TELE:
ConnectionId=[0xE28B6D1D 0x3D9011D6 0x800400D00xBA0D97A1]
IncomingConnectionId=[0xE28B6D1D 0x3D9011D6 0x800400D0 0xBA0D97A1]
CallID=2
Port=3/0/0 (1)
BearerChannel=3/0/0.2
TxDuration=59080 ms
VoiceTxDuration=29790 ms
FaxTxDuration=0 ms
CoderTypeRate=g729r8
NoiseLevel=-54
ACOMLevel=16
OutSignalLevel=-57
InSignalLevel=-51
InfoActivity=1
ERLLevel=16
EchoCancellerMaxReflector=8
SessionTarget= ImgPages=0 CallerName=
CallerIDBlocked=False
AlertTimepoint=1073340 ms
OriginalCallingNumber=9193927582
OriginalCallingOctet=0x21
OriginalCalledNumber=93615494
OriginalCalledOctet=0xC1
OriginalRedirectCalledNumber=
OriginalRedirectCalledOctet=0xFF
TranslatedCallingNumber=9193927582
TranslatedCallingOctet=0x21
TranslatedCalledNumber=93615494
TranslatedCalledOctet=0xC1
TranslatedRedirectCalledNumber=
TranslatedRedirectCalledOctet=0xFF
GwReceivedCalledNumber=93615494
GwReceivedCalledOctet3=0xC1
GwOutpulsedCalledNumber=93615494
GwOutpulsedCalledOctet3=0xC1
GwReceivedCallingNumber=9193927582
```

```
GwReceivedCallingOctet3=0x21
GwReceivedCallingOctet3a=0x81
GwOutpulsedCallingNumber=9193927582
GwOutpulsedCallingOctet3=0x21
GwOutpulsedCallingOctet3a=0x81
DSPIdentifier=3/1:1
Telephony call-legs: 1
SIP call-legs: 0
H323 call-legs: 1
Call agent controlled call-legs: 0
SCCP call-legs: 0
Multicast call-legs: 0
Total call-legs: 2
```

The first table above and the table below describe the significant fields shown in the display, in alphabetical order.

Table 19: show call active voice Field Descriptions

Field	Description
CallDuration	Length of the call, in hours, minutes, and seconds, hh:mm:ss.
CallState	Current state of the call.
Call agent controlled call-legs	Displays call legs for devices that are not telephony endpoints; for example, transcoding and conferencing
ChargedUnits	Total number of charging units that apply to this peer since system startup. The unit of measure for this field is hundredths of second.
CodecBytes	Payload size, in bytes, for the codec used.
CoderTypeRate	Negotiated coder rate. This value specifies the send rate of voice or fax compression to its associated call leg for this call.
ConnectionId	Global call identifier for this gateway call.
ConnectTime	Time, in ms, during which the call was connected.
EchoCancellerMaxReflector	Size of the largest reflector, in ms. The reflector size cannot exceed the configured echo path capacity. For example, if 32 ms is configured, the reflector does not report capacity beyond 32 ms.
ERLLevel	Current echo return loss (ERL) level for this call.
FaxTxDuration	Duration, in ms, of fax transmission from this peer to the voice gateway for this call. You can derive the Fax Utilization Rate by dividing the FaxTxDuration value by the TxDuration value.
GapFillWithInterpolation	Duration, in ms, of a voice signal played out with a signal synthesized from parameters, or samples of data preceding and following in time because voice data was lost or not received in time from the voice gateway for this call.

Field	Description
GapFillWithRedundancy	Duration, in ms, of a voice signal played out with a signal synthesized from available redundancy parameters because voice data was lost or not received in time from the voice gateway for this call.
GapFillWithPrediction	Duration, in ms, of the voice signal played out with a signal synthesized from parameters, or samples of data preceding in time, because voice data was lost or not received in time from the voice gateway for this call. Examples of such pullout are frame-eraser and frame-concealment strategies in G.729 and G.723.1 compression algorithms.
GapFillWithSilence	Duration, in ms, of a voice signal replaced with silence because voice data was lost or not received in time for this call.
GENERIC	Generic or common parameters; that is, parameters that are common for VoIP and telephony call legs.
H320CallType	Total H320 call types available.
H323 call-legs	Total H.323 call legs for which call records are available.
HiWaterPlayoutDelay	High-water-mark voice playout first in first out (FIFO) delay during this call, in ms.
Index	Dial peer identification number.
InfoActivity	Active information transfer activity state for this call.
InfoType	Information type for this call; for example, voice, speech, or fax.
InSignalLevel	Active input signal level from the telephony interface used by this call.
LogicalIfIndex	Index number of the logical interface for this call.
LoWaterPlayoutDelay	Low-water-mark voice playout FIFO delay during this call, in ms.
Media	Medium over which the call is carried. If the call is carried over the (telephone) access side, the entry is TELE. If the call is carried over the voice network side, the entry is either ATM, Frame Relay (FR), or High-Level Data Link Control (HDLC).
Multicast call-legs	Total multicast call legs for which call records are available.
NoiseLevel	Active noise level for this call.
OnTimeRvPlayout	Duration of voice playout from data received on time for this call. Derive the Total Voice Playout Duration for Active Voice by adding the OnTimeRvPlayout value to the GapFill values.
OutSignalLevel	Active output signal level to the telephony interface used by this call.
PeerAddress	Destination pattern or number associated with this peer.
PeerId	ID value of the peer table entry to which this call was made.

Field	Description
PeerIfIndex	Voice port index number for this peer. For ISDN media, this would be the index number of the B channel used for this call.
PeerSubAddress	Subaddress when this call is connected.
ReceiveBytes	Number of bytes received by the peer during this call.
ReceiveDelay	Average playout FIFO delay plus the decoder delay during this voice call, in ms.
ReceivePackets	Number of packets received by this peer during this call.
RemoteIPAddress	Remote system IP address for the VoIP call.
RemoteUDPPort	Remote system User Datagram Protocol (UDP) listener port to which voice packets are sent.
RoundTripDelay	Voice packet round-trip delay, in ms, between the local and remote systems on the IP backbone for this call.
SCCP call-legs	Call legs for SCCP telephony endpoints.
SelectedQoS	Selected Resource Reservation Protocol (RSVP) quality of service (QoS) for this call.
SessionIDLocaluuid	UUID generated from the originating user agent.
SessionIDRemoteuuid	UUID generated from the terminating user agent.
SessionProtocol	Session protocol used for an Internet call between the local and remote routers through the IP backbone.
SessionTarget	Session target of the peer used for this call.
SetupTime	Value of the system UpTime, in ms, when the call associated with this entry was started.
SIP call-legs	Total SIP call legs for which call records are available.
Telephony call-legs	Total telephony call legs for which call records are available.
Total call-legs	Total number of call legs for the call.
TransmitBytes	Number of bytes sent by this peer during this call.
TransmitPackets	Number of packets sent by this peer during this call.
TxDuration	The length of the call. Appears only if the medium is TELE.
VAD	Whether voice activation detection (VAD) was enabled for this call.
VoiceTxDuration	Duration of voice transmission from this peer to the voice gateway for this call, in ms. Derive the Voice Utilization Rate by dividing the VoiceTxDuration value by the TxDuration value.

The following is sample output from the **show call active voice** command for voice traffic over call-agent controlled call legs. Note that call legs for SCCP telephony endpoints, that is, phones controlled by STCAPP, are displayed under the "Call agent controlled call-legs" field ("SCCP call-legs" displays call legs for devices that are not telephony endpoints; for example, transcoding and conferencing).

```
Router# show call active voice
Telephony call-legs: 2
SIP call-legs: 0
H323 call-legs: 0
Call agent controlled call-legs: 2
SCCP call-legs: 0
Multicast call-legs: 0
Total call-legs: 4
 GENERIC:
SetupTime=1557650 ms
Index=1
PeerAddress=
PeerSubAddress=
PeerId=999100
PeerIfIndex=14
LogicalIfIndex=10
ConnectTime=1562040 ms
CallDuration=00:01:01 sec
CallState=4
CallOrigin=2
ChargedUnits=0
InfoType=speech
TransmitPackets=3101
TransmitBytes=519564
ReceivePackets=3094
ReceiveBytes=494572
TELE:
ConnectionId=[0x11B1860C 0x22D711D7 0x8014E4D4 0x8FD15327]
IncomingConnectionId=[0x11B1860C 0x22D711D7 0x8014E4D4 0x8FD15327]
CallID=25
Port=3/0/0 (25)
BearerChannel=3/0/0.1
TxDuration=59670 ms
VoiceTxDuration=59670 ms
FaxTxDuration=0 ms
CoderTypeRate=g711ulaw
NoiseLevel=-12
ACOMLevel=22
OutSignalLevel=-12
InSignalLevel=-11
InfoActivity=1
ERLLevel=22
EchoCancellerMaxReflector=2
SessionTarget=
ImgPages=0
CallerName=
CallerIDBlocked=False
OriginalCallingNumber=
OriginalCallingOctet=0x0
OriginalCalledNumber=
OriginalCalledOctet=0x80
OriginalRedirectCalledNumber=
OriginalRedirectCalledOctet=0x0
TranslatedCallingNumber=
TranslatedCallingOctet=0x0
TranslatedCalledNumber=
```

```
TranslatedCalledOctet=0x80
TranslatedRedirectCalledNumber=
TranslatedRedirectCalledOctet=0x0
DSPIdentifier=1/1:1
 GENERIC:
SetupTime=1559430 ms
Index=1
PeerAddress=7702
PeerSubAddress=
PeerId=999100
PeerIfIndex=14
LogicalIfIndex=11
ConnectTime=1562020 ms
CallDuration=00:01:03 sec
CallState=4
CallOrigin=1
ChargedUnits=0
InfoType=speech
TransmitPackets=3151
TransmitBytes=528900
ReceivePackets=3158
ReceiveBytes=503876
TELE:
ConnectionId=[0x0 0x0 0x0 0x0]
IncomingConnectionId=[0x0 0x0 0x0 0x0]
CallID=26
Port=3/0/0 (26)
BearerChannel=3/0/0.2
TxDuration=60815 ms
VoiceTxDuration=60815 ms
FaxTxDuration=0 ms
CoderTypeRate=g711ulaw
NoiseLevel=-12
ACOMLevel=28
OutSignalLevel=-12
InSignalLevel=-11
InfoActivity=1
ERLLevel=28
EchoCancellerMaxReflector=2
SessionTarget=
ImgPages=0
CallerName=
CallerIDBlocked=False
AlertTimepoint=1559430 ms
OriginalCallingNumber=
OriginalCallingOctet=0x0
OriginalCalledNumber=
OriginalCalledOctet=0x0
OriginalRedirectCalledNumber=
OriginalRedirectCalledOctet=0x0
TranslatedCallingNumber=7701
TranslatedCallingOctet=0x0
TranslatedCalledNumber=7702
TranslatedCalledOctet=0x0
TranslatedRedirectCalledNumber=
TranslatedRedirectCalledOctet=0x0
GwOutpulsedCalledNumber=7702
GwOutpulsedCalledOctet3=0x0
GwOutpulsedCallingNumber=7701
GwOutpulsedCallingOctet3=0x0
GwOutpulsedCallingOctet3a=0x0
DSPIdentifier=1/1:2
 GENERIC:
SetupTime=1562040 ms
```

```
Index=1
PeerAddress=
PeerSubAddress=
PeerId=0
PeerIfIndex=0
LogicalIfIndex=0
ConnectTime=0 ms
CallDuration=00:00:00 sec
CallState=2
CallOrigin=1
ChargedUnits=0
InfoType=speech
TransmitPackets=3215
TransmitBytes=512996
ReceivePackets=3208
ReceiveBytes=512812
VOIP:
ConnectionId[0x0 0x0 0x0 0x0]
IncomingConnectionId[0x0 0x0 0x0 0x0]
CallID=27
RemoteIPAddress=10.10.0.0
RemoteUDPPort=17718
RemoteSignallingIPAddress=10.10.0.0
RemoteSignallingPort=0
RemoteMediaIPAddress=10.2.6.10
RemoteMediaPort=17718
RoundTripDelay=0 ms
SelectedQoS=best-effort
tx_DtmfRelay=inband-voice
FastConnect=FALSE
AnnexE=FALSE
Separate H245 Connection=FALSE
H245 Tunneling=FALSE
SessionProtocol=other
ProtocolCallId=
SessionTarget=
OnTimeRvPlayout=60640
GapFillWithSilence=0 ms
GapFillWithPrediction=0 ms
GapFillWithInterpolation=0 ms
GapFillWithRedundancy=0 ms
HiWaterPlayoutDelay=105 ms
LoWaterPlayoutDelay=105 ms
TxPakNumber=3040
TxSignalPak=0
TxComfortNoisePak=0
TxDuration=60815
TxVoiceDuration=60815
RxPakNumber=3035
RxSignalPak=0
RxDuration=0
TxVoiceDuration=60690
VoiceRxDuration=60640
RxOutOfSeq=0
RxLatePak=0
RxEarlyPak=0
PlayDelayCurrent=105
PlayDelayMin=105
PlayDelayMax=105
PlayDelayClockOffset=-1662143961
PlayDelayJitter=0
PlayErrPredictive=0
PlayErrInterpolative=0
PlayErrSilence=0
```

```
PlayErrBufferOverFlow=0
PlayErrRetroactive=0
PlayErrTalkspurt=0
OutSignalLevel=-12
InSignalLevel=-11
LevelTxPowerMean=0
LevelRxPowerMean=-115
LevelBgNoise=0
ERLLevel=28
ACOMLevel=28
ErrRxDrop=0
ErrTxDrop=0
ErrTxControl=0
ErrRxControl=0
PlayoutMode = undefined
PlayoutInitialDelay=0 ms
ReceiveDelay=105 ms
LostPackets=0
EarlyPackets=0
LatePackets=0
SRTP = off
VAD = disabled
CoderTypeRate=g711ulaw
CodecBytes=160
Media Setting=flow-around
Modem passthrough signaling method is nse:
Buffer Fill Events = 0
Buffer Drain Events = 0
Percent Packet Loss = 0
Consecutive-packets-lost Events = 0
Corrected packet-loss Events = 0
Last Buffer Drain/Fill Event = 0sec
Time between Buffer Drain/Fills = Min 0sec Max 0sec
CallerName=
CallerIDBlocked=False
OriginalCallingNumber=
OriginalCallingOctet=0x0
OriginalCalledNumber=
OriginalCalledOctet=0x0
OriginalRedirectCalledNumber=
OriginalRedirectCalledOctet=0x0
TranslatedCallingNumber=
TranslatedCallingOctet=0x0
TranslatedCalledNumber=
TranslatedCalledOctet=0x0
TranslatedRedirectCalledNumber=
TranslatedRedirectCalledOctet=0x0
MediaInactiveDetected=no
MediaInactiveTimestamp=
MediaControlReceived=
Username=
 GENERIC:
SetupTime=1562040 ms
Index=2
PeerAddress=
PeerSubAddress=
PeerId=0
PeerIfIndex=0
LogicalIfIndex=0
ConnectTime=0 ms
CallDuration=00:00:00 sec
CallState=2
CallOrigin=1
ChargedUnits=0
```

```
InfoType=speech
TransmitPackets=3380
TransmitBytes=540332
ReceivePackets=3386
ReceiveBytes=540356
VOIP:
ConnectionId[0x0 0x0 0x0 0x0]
IncomingConnectionId[0x0 0x0 0x0 0x0]
CallID=28
RemoteIPAddress=10.0.0.0
RemoteUDPPort=18630
RemoteSignallingIPAddress=10.10.0.0
RemoteSignallingPort=0
RemoteMediaIPAddress=10.2.6.10
RemoteMediaPort=18630
RoundTripDelay=0 ms
SelectedQoS=best-effort
tx_DtmfRelay=inband-voice
FastConnect=FALSE
AnnexE=FALSE
Separate H245 Connection=FALSE
H245 Tunneling=FALSE
SessionProtocol=other
ProtocolCallId=
SessionTarget=
OnTimeRvPlayout=63120
GapFillWithSilence=0 ms
GapFillWithPrediction=0 ms
GapFillWithInterpolation=0 ms
GapFillWithRedundancy=0 ms
HiWaterPlayoutDelay=105 ms
LoWaterPlayoutDelay=105 ms
TxPakNumber=3158
TxSignalPak=0
TxComfortNoisePak=0
TxDuration=63165
TxVoiceDuration=63165
RxPakNumber=3164
RxSignalPak=0
RxDuration=0
TxVoiceDuration=63165
VoiceRxDuration=63120
RxOutOfSeq=0
RxLatePak=0
RxEarlyPak=0
PlayDelayCurrent=105
PlayDelayMin=105
PlayDelayMax=105
PlayDelayClockOffset=957554296
PlayDelayJitter=0
PlayErrPredictive=0
PlayErrInterpolative=0
PlayErrSilence=0
PlayErrBufferOverFlow=0
PlayErrRetroactive=0
PlayErrTalkspurt=0
OutSignalLevel=-12
InSignalLevel=-11
LevelTxPowerMean=0
LevelRxPowerMean=-114
LevelBgNoise=0
ERLLevel=22
ACOMLevel=22
ErrRxDrop=0
```

```
ErrTxDrop=0
ErrTxControl=0
ErrRxControl=0
PlayoutMode = undefined
PlayoutInitialDelay=0 ms
ReceiveDelay=105 ms
LostPackets=0
EarlyPackets=0
LatePackets=0
SRTP = off
VAD = disabled
CoderTypeRate=g711ulaw
CodecBytes=160
Media Setting=flow-around
Modem passthrough signaling method is nse:
Buffer Fill Events = 0
Buffer Drain Events = 0
Percent Packet Loss = 0
Consecutive-packets-lost Events = 0
Corrected packet-loss Events = 0
Last Buffer Drain/Fill Event = 0sec
Time between Buffer Drain/Fills = Min 0sec Max 0sec
CallerName=
CallerIDBlocked=False
OriginalCallingNumber=
OriginalCallingOctet=0x0
OriginalCalledNumber=
OriginalCalledOctet=0x0
OriginalRedirectCalledNumber=
OriginalRedirectCalledOctet=0x0
TranslatedCallingNumber=
TranslatedCallingOctet=0x0
TranslatedCalledNumber=
TranslatedCalledOctet=0x0
TranslatedRedirectCalledNumber=
TranslatedRedirectCalledOctet=0x0
MediaInactiveDetected=no
MediaInactiveTimestamp=
MediaControlReceived=
Username=
Telephony call-legs: 2
SIP call-legs: 0
H323 call-legs: 0
Call agent controlled call-legs: 2
SCCP call-legs: 0
Multicast call-legs: 0
Total call-legs: 4
```

The tables above describe the significant fields shown in the display, in alphabetical order.

The following is sample output from the **show call active voice** command to indicate if Service Advertisement Framework (SAF) is being used:

```
Router# show call active voice
Total call-legs: 2
GENERIC:
SetupTime=1971780 ms
Index=1
PeerAddress=6046692010
PeerSubAddress=
PeerId=20003
PeerIfIndex=17
.
.
```

```
.
VOIP:
SessionProtocol=sipv2
ProtocolCallId=7A9E7D9A-EAD311DC-8036BCC4-6EEE85D6@1.5.6.12
SessionTarget=1.5.6.10
SafEnabled=TRUE
SafTrunkRouteId=1
SafPluginDialpeerTag=8
```

The tables above describe the significant fields shown in the display.

The following is sample output from the **show call active voice** command for fax-relay traffic:

```
Router# show call active voice
Telephony call-legs: 0
SIP call-legs: 0
H323 call-legs: 1
MGCP call-legs: 0
Multicast call-legs: 0
Total call-legs: 1
 GENERIC:
SetupTime=1049400 ms
Index=2
PeerAddress=52930
PeerSubAddress=
PeerId=82
PeerIfIndex=222
LogicalIfIndex=0
ConnectTime=105105
CallDuration=00:00:59
CallState=4
CallOrigin=1
ChargedUnits=0
InfoType=10
TransmitPackets=1837
TransmitBytes=29764
ReceivePackets=261
ReceiveBytes=4079
VOIP:
ConnectionId[0xEB630F4B 0x9F5E11D7 0x8008CF18 0xB9C3632]
IncomingConnectionId[0xEB630F4B 0x9F5E11D7 0x8008CF18 0xB9C3632]
RemoteIPAddress=10.7.95.3
RemoteUDPPort=16610
RemoteSignallingIPAddress=10.7.95.3
RemoteSignallingPort=1720
RemoteMediaIPAddress=10.7.95.3
RemoteMediaPort=16610
RoundTripDelay=13 ms
SelectedQoS=best-effort
tx_DtmfRelay=inband-voice
FastConnect=TRUE
AnnexE=FALSE
Separate H245 Connection=FALSE
H245 Tunneling=TRUE
SessionProtocol=cisco
ProtocolCallId=
SessionTarget=ipv4:10.7.95.3
OnTimeRvPlayout=1000
GapFillWithSilence=0 ms
GapFillWithPrediction=0 ms
GapFillWithInterpolation=0 ms
GapFillWithRedundancy=0 ms
HiWaterPlayoutDelay=110 ms
LoWaterPlayoutDelay=70 ms
```

```
ReceiveDelay=70 ms
LostPackets=0
EarlyPackets=1
LatePackets=0
VAD = enabled
CoderTypeRate=t38
CodecBytes=40
Media Setting=flow-through
AlertTimepoint=104972
CallerName=
CallerIDBlocked=False
OriginalCallingNumber=4085550130
OriginalCallingOctet=0x0
OriginalCalledNumber=52930
OriginalCalledOctet=0xE9
OriginalRedirectCalledNumber=
OriginalRedirectCalledOctet=0x7F
TranslatedCallingNumber=4085550130
TranslatedCallingOctet=0x0
TranslatedCalledNumber=52930
TranslatedCalledOctet=0xE9
TranslatedRedirectCalledNumber=
TranslatedRedirectCalledOctet=0xFF
GwReceivedCalledNumber=52930
GwReceivedCalledOctet3=0xE9
GwOutpulsedCalledNumber=52930
GwOutpulsedCalledOctet3=0xE9
GwReceivedCallingNumber=555-0100
GwReceivedCallingOctet3=0x0
GwReceivedCallingOctet3a=0x80
GwOutpulsedCallingNumber=555-0101
GwOutpulsedCallingOctet3=0x0
GwOutpulsedCallingOctet3a=0x80
Username=
FaxRelayMaxJitterBufDepth  = 0 ms
FaxRelayJitterBufOverFlow = 0
FaxRelayHSmodulation = 0
FaxRelayNumberOfPages = 0
Telephony call-legs: 0
SIP call-legs: 0
H323 call-legs: 1
MGCP call-legs: 0
Multicast call-legs: 0
Total call-legs: 1
```

The tables above describe the significant fields shown in the display.

The following is sample output from the **show call active voice brief** command:

```
Router# show call active voice brief

<ID>: <CallID> <start>ms.<index> (<start>) +<connect> pid:<peer_id> <dir> <addr> <state>
  dur hh:mm:ss tx:<packets>/<bytes> rx:<packets>/<bytes> dscp:<packets violation>
media:<packets
violation> audio tos:<audio tos value> video tos:<video tos value>
 IP <ip>:<udp> rtt:<time>ms pl:<play>/<gap>ms lost:<lost>/<early>/<late>
  delay:<last>/<min>/<max>ms <codec> <textrelay> <transcoded

 media inactive detected:<y/n> media cntrl rcvd:<y/n> timestamp:<time>

 long duration call detected:<y/n> long duration call duration :<sec> timestamp:<time>
 LostPacketRate:<%> OutOfOrderRate:<%>
 LocalUUID:<%> RemoteUUID:<%>
 VRF:<%>
```

```
 MODEMPASS <method> buf:<fills>/<drains> loss <overall%> <multipkt>/<corrected>
  last <buf event time>s dur:<Min>/<Max>s
FR <protocol> [int dlci cid] vad:<y/n> dtmf:<y/n> seq:<y/n>
 <codec> (payload size)
ATM <protocol> [int vpi/vci cid] vad:<y/n> dtmf:<y/n> seq:<y/n>
 <codec> (payload size)
Tele <int> (callID) [channel_id] tx:<tot>/<v>/<fax>ms <codec> noise:<l> acom:<l> i/o:<l>/<l>
dBm
 MODEMRELAY info:<rcvd>/<sent>/<resent> xid:<rcvd>/<sent> total:<rcvd>/<sent>/<drops>
        speeds(bps): local <rx>/<tx> remote <rx>/<tx>
Proxy <ip>:<audio udp>,<video udp>,<tcp0>,<tcp1>,<tcp2>,<tcp3> endpt: <type>/<manf>
bw: <req>/<act> codec: <audio>/<video>
 tx: <audio pkts>/<audio bytes>,<video pkts>/<video bytes>,<t120 pkts>/<t120 bytes>
rx: <audio pkts>/<audio bytes>,<video pkts>/<video bytes>,<t120 pkts>/<t120 bytes>


Telephony call-legs: 0
SIP call-legs: 2
H323 call-legs: 0
Call agent controlled call-legs: 0
SCCP call-legs: 0
Multicast call-legs: 0
Total call-legs: 2
1218 : 15 2442930ms.1 (*13:22:20.797 UTC Thu Feb 18 2016) +2010 pid:880 Answer sipp active
 dur 00:00:02 tx:0/0 rx:0/0 dscp:0 media:0 audio tos:0xB8 video tos:0x0
 IP 1.4.186.60:6005 SRTP: off rtt:0ms pl:0/0ms lost:0/0/0 delay:0/0/0ms g711ulaw TextRelay:
 off
Transcoded: No ICE: Off
 media inactive detected:n media contrl rcvd:n/a timestamp:n/a
 long duration call detected:n long duration call duration:n/a timestamp:n/a
 LostPacketRate:0.00 OutOfOrderRate:0.00
LocalUUID:ab30317f1a784dc48ff824d0d3715d86
RemoteUUID:47755a9de7794ba387653f2099600ef2
 VRF: VRF1
1218 : 16 2442940ms.1 (*13:22:20.807 UTC Thu Feb 18 2016) +2000 pid:770 Originate 7777
active
 dur 00:00:02 tx:0/0 rx:0/0 dscp:0 media:0 audio tos:0xB8 video tos:0x0
 IP 9.45.33.11:16384 SRTP: off rtt:0ms pl:0/0ms lost:0/0/0 delay:0/0/0ms g711ulaw TextRelay:
 off
Transcoded: No ICE: Off
 media inactive detected:n media contrl rcvd:n/a timestamp:n/a
 long duration call detected:n long duration call duration:n/a timestamp:n/a
 LostPacketRate:0.00 OutOfOrderRate:0.00
LocalUUID:47755a9de7794ba387653f2099600ef2
RemoteUUID:ab30317f1a784dc48ff824d0d3715d86
 VRF: NA

Telephony call-legs: 0
SIP call-legs: 2
H323 call-legs: 0
Call agent controlled call-legs: 0
SCCP call-legs: 0
Multicast call-legs: 0
Total call-legs: 2
```

The following is an example of the **show call active voice** command using the **echo-canceller** keyword. The number 9 represents the hexadecimal ID of an active voice call.

```
Router# show call active voice echo-canceller 9
ACOM=-65  ERL=45
Echo canceller control words=6C 0
Bypass=OFF  Tail=64  Residual ecan=Comfort noise
```

```
Freeze=OFF  Modem tone disable=Ignore 2100Hz tone
Worst ERL=6  High level compensation=OFF
Max amplitude reflector (in msec)=5
Ecan version = 8180
```

The following is sample output from the **show call active voice echo-canceller** command for a call with a hexadecimal ID of 10:

```
Router# show call active voice echo-canceller 10

ACOM=-15  ERL=7
Echo canceller control words=6C 0
Bypass=OFF  Tail=64  Residual ecan=Comfort noise
Freeze=OFF  Modem tone disable=Ignore 2100Hz tone
Worst ERL=6  High level compensation=OFF
Max amplitude reflector (in msec)=64
```

The call ID number (which is 10 in the preceding example) changes with every new active call. When an active call is up, you must enter the **show call active voice brief** command to obtain the call ID number. The call ID must be converted to hexadecimal value if you want to use the **show call active voice echo-canceller** *x* command (*x* = call ID converted to hexadecimal value).

The table below shows call ID examples converted to hexadecimal values (generally incremented by 2):

Table 20: Call IDs Converted to Hex

Decimal	Hex
2	2
4	4
6	6
8	8
10	A
12	C

Alternatively, you can use the **show voice call status** command to obtain the call ID. The call ID output is already in hexadecimal values form when you use this command:

```
Router# show voice call status

CallID     CID  ccVdb      Port      DSP/Ch  Called #   Codec    Dial-peers
0x1        11CE 0x02407B20 1:0.1     1/1     1000       g711ulaw 2000/1000
```

The following is sample output from the **show call active voice** command using the **compact** keyword:

```
Router# show call active voice compact
<callID>  A/O  FAX T<sec>   Codec      type    Peer        Address IP R<ip>:<udp>  VRF
Total call-legs: 2
8565722  ANS    T12         g711ulaw   VOIP   P777412373   10.0.0.1:30804          VRF1
8565723  ORG    T12         g711ulaw   VOIP   P777512373   11.0.0.1:30804          VRF2
```

The following is sample output from the **show call active voice redirect** command using the **tbct** keyword:

```
Router# show call active voice redirect tbct
TBCT:
        Maximum no. of TBCT calls allowed:No limit
        Maximum TBCT call duration:No limit
Total number TBCT calls currently being monitored = 1
ctrl name=T1-2/0, tag=13, call-ids=(7, 8), start_time=*00:12:25.985 UTC Mon Mar 1 1993
```

The table below describes the significant fields shown in the display.

Table 21: show call active voice redirect Field Descriptions

Field	Description
Maximum no. of TBCT calls allowed	Maximum number of calls that can use TBCT as defined by the **tbct max calls** command.
Maximum TBCT call duration	Maximum length allowed for a TBCT call as defined by the **tbct max call-duration** command.
Total number TBCT calls currently being monitored	Total number of active TBCT calls.
ctrl name	Name of the T1 controller where the call originated.
tag	Call tag number that identifies the call.
call-ids	Numbers that uniquely identify the call legs.
start_time	Time, in hours, minutes, and seconds, when the redirected call began.

Related Commands

Command	Description
show call active fax	Displays call information for fax transmissions that are in progress.
show call history	Displays the call history table.
show call-router routes	Displays the dynamic routes in the cache of the BE.
show call-router status	Displays the Annex G BE status.
show dial-peer voice	Displays configuration information for dial peers.
show num-exp	Displays how the number expansions are configured in VoIP.
show voice call status	Displays the call status for voice ports on the Cisco router or concentrator.
show voice port	Displays configuration information about a specific voice port.

show call application app-level

To display application-level statistics for voice applications, use the **show call application app-level**command in privileged EXEC mode.

show call application {**active** | **history**} **app-level** [**app-tag** *application-name* | **summary**]

Syntax Description

active	Displays statistics for active application instances.
history	Displays statistics for terminated application instances.
app-tag *application-name*	Name of a specific voice application. Output displays statistics for that voice application.
summary	Displays a summary for each application.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.3(8)T	This command was introduced.

Usage Guidelines

- To display statistics with this command, you must enable statistics collection with the **call application stats** command.
- This command displays gauges and counters that are aggregated per application. The values represent all instances of a particular voice application running on the gateway while statistics collection is enabled.
- To reset application-level counters to zero and subtract the counters from the gateway-level statistics in history, use the **clear call application stats** command. Statistic counters continue accumulating in history until you use the **clear call application stats** command or the gateway reloads.

Note Statistics for an application are automatically cleared if the application is deleted with the **no call application voice** command or its script is reloaded with the **call application voice load** command.

Examples

The following is sample output from the **show call application app-level** command using different keywords:

```
Router# show call application active app-level summary
Application level active Info:
                              Sessions
App Name                  w/ Stats   Total
session                   0          0
fax_hop_on                0          0
clid_authen               0          0
clid_authen_collect       0          0
```

```
clid_authen_npw          0          0
clid_authen_col_npw      0          0
clid_col_npw_3           0          0
clid_col_npw_npw         0          0
Default                  0          0
lib_off_app              0          0
fax_on_vfc_onramp_app    0          0
asr                      0          0
offramp                  0          0
generic                  1          1
smtp_record              0          0
authen                   0          0
authorize                0          0
ram_record_replay        0          0
Router# show call application active app-level app-tag generic

Application level active Info:
Application Name:              generic
url:                           tftp://10.10.10.113/tftplocal/generic.vxml
Total sessions:                                  1
Sessions w/ stats:                               1
Currently connected incoming PSTN legs:          1
Currently connected outgoing PSTN legs:          0
Currently connected incoming VoIP legs:          0
Currently connected outgoing VoIP legs:          0
Placecalls in transit:                           0
Handouts in transit:                             0
Pending ASNL subscriptions:                      0
Pending ASNL unsubscriptions:                    0
Prompts playing (non-TTS):                       0
Recordings:                                      0
TTS prompts playing:                             0
```

For a description of the fields shown in the display above, see Table 38 on page 1363.

```
Router# show call application history app-level summary

Application level history Info:
                                  Sessions                      Last Reset
App Name                 Stats w/ Stats   Total      Errors     Time
session                  N     0          0          0
fax_hop_on               N     0          0          0
clid_authen              N     0          0          0
clid_authen_collect      N     0          0          0
clid_authen_npw          N     0          0          0
clid_authen_col_npw      N     0          0          0
clid_col_npw_3           N     0          0          0
clid_col_npw_npw         N     0          0          0
Default                  N     0          0          0
lib_off_app              N     0          0          0
fax_on_vfc_onramp_app    N     0          0          0
ram_record_replay        N     0          0          0
authorize                N     0          0          0
authen                   N     0          0          0
smtp_record              N     0          0          0
generic                  Y     2          2          4          *Jul  3 15:49:28
offramp                  N     0          0          0
asr                      N     0          0          0
```

The table below describes the fields shown in the display.

Table 22: show call application history app-level Field Descriptions

Field	Description
App Name	Name of the voice application.
Stats	Whether statistics is enabled for this application. **Note** If statistics is enabled, this field displays N until there is at least one active instance of the application.
Sessions w/ stats	Number of terminated application instances that the gauges represent.
Total	Total number of instances of the application.
Errors	Total number of errors for all instances of the application.
Last Reset Time	Time at which the statistics were last cleared with the **clear call application stats** command, or the gateway was restarted.

```
Router# show call application history app-level app-tag generic

Application level history Info:
Application name:              generic
URL:                           tftp://10.10.10.113/tftplocal/generic.vxml
Total sessions:                2
Sessions w/ stats:             2
Last reset time:               *Jul  3 15:49:28 PST
Statistics:
 Subscriber Service - Call
                                                PSTN                VOIP
                                        Incoming Outgoing  Incoming Outgoing
Legs setup:                             2        0         0        0
Total legs connected:                   2        0         0        0
Legs handed in:                         0        0         0        0
Legs handed in returned back:           0        0         0        0
Legs handed out:                        0        0         0        0
Legs handed out came back:              0        0         0        0
Legs disconnected normally:             2        0         0        0
Legs disconnected for user error:       0        0         0        0
Legs disconnected for system error:     0        0         0        0
 Subscriber Service - Media
                                        Play       Record     TTS
Media attempts:                         3          0          0
Media successes:                        0          0          0
Media aborts:                           0          0          0
Media failures:                         3          0          0
Total media duration (in seconds):      3          0          0
 Application Internal Service - Handoff
                                        Incoming   Outgoing
Bridged handoffs:                       0          0
Bridged handoffs returned:              0          0
Blind handoffs:                         0          0
Handoffs failed:                        x          0
 Application Internal Service - Placecall/transfer
Placecall requests:                     0
Placecall successes:                    0
Placecall failures:                     0
 Application Internal Service - Document Read-Write
```

```
                                        Read       Write
Doc requests:                           0          0
Doc successes:                          0          0
Doc failures:                           0          0
 Application Internal Service - Downloaded Script
Script parse errors:                    0
 Application Internal Service - ASNL
ASNL notifications:                     0
                                        Subscription   Unsubscription
ASNL requests:                          0              0
ASNL successes:                         0              0
ASNL failures:                          0              0
 Subscriber Interaction - DTMF
DTMFs not matched:                      0
DTMFs matched:                          0
DTMFs no input:                         1
DTMFs long pound:                       0
Subscriber Interaction - ASR
ASRs not matched:                       0
ASRs matched:                           0
ASRs no input:                          0
 Subscriber Interaction - AAA
                                        Authentication Authorization
AAA successes:                          0              1
AAA failures:                           0              0
```

For a description of the fields shown in this display, see Table 41 on page 1379.

Related Commands

Command	Description
call application event-log	Enables event logging for voice application instances.
call application stats	Enables statistics collection for voice applications.
call application voice event-log	Enables event logging for a specific voice application.
clear call application stats	Clears application-level statistics in history and subtracts the statistics from the gateway-level statistics.
show call application gateway-level	Displays gateway-level statistics for voice application instances.
show call application session-level	Displays event logs and statistics for voice application instances.

show call application gateway-level

To display gateway-level statistics for voice application instances, use the **show call application gateway-level** command in privileged EXEC mode.

show call application {**active** | **history**} **gateway-level**

Syntax Description

active	Displays statistics for active application instances.
history	Displays statistics for terminated application instances.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.3(8)T	This command was introduced.

Usage Guidelines

- To display statistics with this command, you must enable statistics collection with the **call application stats** command.
- This command displays gauges and counters that are aggregated per gateway. The values represent all instances of all voice applications running on the gateway while statistics collection is enabled.
- To reset application-level counters to zero and subtract the counters from the gateway-level statistics in history, use the **clear call application stats** command. Statistic counters continue accumulating in history until you use the **clear call application stats** command or the gateway reloads.

Note Statistics for an application are automatically cleared if the application is deleted with the **no call application voice** command or its script is reloaded with the **call application voice load** command.

Examples

The following is sample output from the **show call application gateway-level** command using different keywords:

```
Router# show call application active gateway-level
Gateway level statistics for active application sessions:
Sessions w/ stats:                              1
Currently connected incoming PSTN legs:         1
Currently connected outgoing PSTN legs:         0
Currently connected incoming VoIP legs:         0
Currently connected outgoing VoIP legs:         0
Placecalls in transit:                          0
Handouts in transit:                            0
Pending ASNL subscriptions:                     0
Pending ASNL unsubscriptions:                   0
Prompts playing (non-TTS):                      0
Recordings:                                     0
TTS prompts playing:                            0
```

The table below describes the fields shown in the display.

Table 23: show call application active gateway-level Field Descriptions

Field	Description
Sessions w/ stats	Number of active application instances that the gauges represent.
Currently connected incoming PSTN legs	Number of active call legs that are incoming from the PSTN.
Currently connected outgoing PSTN legs	Number of active call legs that are outgoing to the PSTN.
Currently connected incoming VoIP legs	Number of active call legs that are incoming from the IP network.
Currently connected outgoing VoIP legs	Number of active call legs that are outgoing to the IP network.
Placecalls in transit	Number of outgoing calls in progress for all active application instances. The value is decremented by one after the call is either set up or the setup fails.
Handouts in transit	Number of handoffs in progress for all active application instances. The value is decremented by one after the receiving application either hands back the application or rejects the handoff.
Pending ASNL subscriptions	Number of Application Subscribe Notify Layer (ASNL) subscription requests that are in progress for all active application instances.
Pending ASNL unsubscriptions	Number of ASNL unsubscription requests that are in progress for all active application instances.
Prompts playing (non-TTS)	Number of recorded prompts being played in all active application instances.
Recordings	Number of recordings being made in all active application instances.
TTS prompts playing	Number of text-to-speech (TTS) prompts playing in all active application instances.

```
Router# show call application history gateway-level

Gateway level statistics for history application sessions:
Sessions w/ stats:             2
Last reset time:               *Jul  3 15:49:28 PST
Statistics:
 Subscriber Service - Call
                                                PSTN                VOIP
                                          Incoming Outgoing  Incoming Outgoing
Legs setup:                               2        0         0        0
Total legs connected:                     2        0         0        0
Legs handed in:                           0        0         0        0
Legs handed in returned back:             0        0         0        0
Legs handed out:                          0        0         0        0
```

```
Legs handed out came back:                0         0         0         0
Legs disconnected normally:               2         0         0         0
Legs disconnected for user error:         0         0         0         0
Legs disconnected for system error:       0         0         0         0
 Subscriber Service - Media
                                          Play      Record    TTS
Media attempts:                           3         0         0
Media successes:                          0         0         0
Media aborts:                             0         0         0
Media failures:                           3         0         0
Total media duration (in seconds):        3         0         0
 Subscriber Interaction - DTMF
DTMFs not matched:                        0
DTMFs matched:                            0
DTMFs no input:                           1
DTMFs long pound:                         0
```

For a description of the fields shown with the **history** keyword, see the table above.

Related Commands

Command	Description
call application stats	Enables statistics collection for voice applications.
clear call application stats	Clears application-level statistics in history and subtracts the statistics from the gateway-level statistics.
show call application app-level	Displays application-level statistics for voice applications.
show call application session-level	Displays event logs and statistics for voice application instances.

show call application interface

To display event logs and statistics for application interfaces, use the **show call application interface**command in privileged EXEC mode.

show call application interface [**summary** | {**aaa** | **asr** | **flash** | **http** | **ram** | **rtsp** | **smtp** | **tftp** | **tts**} [**server** *server*] [**event-log** | **info** | **summary**]]

Syntax Description

summary	(Optional) Displays a short summary of all interface types or the selected interface.
aaa	Authentication, authorization, and accounting (AAA) interface type.
asr	Automatic speech recognition (ASR) interface type.
flash	Flash memory of the Cisco gateway.
http	Hypertext Transfer Protocol (HTTP) interface type.
ram	Memory of the Cisco gateway.
rtsp	Real Time Streaming Protocol (RTSP) interface type.
smtp	Simple Mail Transfer Protocol (SMTP) interface type.
tftp	Trivial File Transfer Protocol (TFTP) interface type.
tts	Text-to-speech (TTS) interface type.
server *server*	(Optional) Displays event logs or statistics for the specified server.
event-log	(Optional) Displays event logs for the selected interface type or server.
info	(Optional) Displays statistics for the selected interface type or server.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.3(8)T	This command was introduced.

Usage Guidelines

If you use the **server** keyword, only statistics or event logs for that server display. To display event logs or statistics with this command, you must enable statistics and event logging with the **call application interface event-log** and **call application interface stats** command, respectively. To reset statistic counters to zero and clear the event logs in history, use the **clear call application interface** command.

Examples

The following is sample output from the **show call application interface** command using different keywords:

```
Router# show call application interface summary
```

```
Aggregated statistics for http service:
Stats last reset time *Jul  3 15:24:48 PST
Read requests:                   3
Read successes:                  0
Read failures:                   3
Read aborts:                     0
Total bytes read:                0
Write requests:                  0
Write successes:                 0
Write failures:                  0
Write aborts:                    0
Total bytes written:             0
Aggregated statistics for tts service:
Stats last reset time *Jul  3 15:24:48 PST
Read requests:                   0
Read successes:                  0
Read failures:                   0
Read aborts:                     0
Aggregated statistics for asr service:
Stats last reset time *Jul  3 15:24:48 PST
Read requests:                   0
Read successes:                  0
Read failures:                   0
Read aborts:                     0
Aggregated statistics for tftp service:
Stats last reset time *Jul  3 15:24:48 PST
Read requests:                   3
Read successes:                  2
Read failures:                   0
Read aborts:                     1
Total bytes read:                145888
Router# show call application interface tftp summary

Aggregated statistics for tftp service:
Stats last reset time *Jul  3 15:24:48 PST
Read requests:                   3
Read successes:                  2
Read failures:                   0
Read aborts:                     1
Total bytes read:                145888
Server Name          Stats Error Count           Event Log
172.19.139.145       Y     0                     Y
speech-serv          Y     0                     N
Router# show call application interface tftp

Server name:         172.19.139.145
Statistics:
Last reset time *Jul  3 16:08:13 PST
Read requests:                   1
Read successes:                  2
Read failures:                   0
Read aborts:                     1
Total bytes read:                145888
Event log:
Last reset time *Jul  3 16:08:13 PST
buf_size=50K, log_lvl=INFO
<ctx_id>:<timestamp>:<seq_no>:<severity>:<msg_body>
172.19.139.145:1057277293:53:INFO: ID = 6549D9E0: Read requested for URL =
tftp://172.19.139.145/audio/ch_welcome.au
172.19.139.145:1057277295:54:INFO: ID = 6549D9E0: Streamed read transaction Successful URL
 = tftp://172.19.139.145/audio/ch_welcome.au
172.19.139.145:1057277306:59:INFO: ID = 649A0320: Streamed read transaction Successful URL
 = tftp://172.19.139.145/audio/ch_welcome.au
172.19.139.145:1057277317:65:INFO: ID = 650922A8: Read request aborted for URL =
```

```
tftp://172.19.139.145/audio/ch_welcome.au
-------------------------------------------------------------------------------
Router# show call application interface tftp event-log

Server name:         172.19.139.145
Event log:
Last reset time *Jul  3 16:08:13 PST
buf_size=50K, log_lvl=INFO
<ctx_id>:<timestamp>:<seq_no>:<severity>:<msg_body>
172.19.139.145:1057277293:53:INFO: ID = 6549D9E0: Read requested for URL =
tftp://172.19.139.145/audio/ch_welcome.au
172.19.139.145:1057277295:54:INFO: ID = 6549D9E0: Streamed read transaction Successful URL
 = tftp://172.19.139.145/audio/ch_welcome.au
172.19.139.145:1057277306:59:INFO: ID = 649A0320: Streamed read transaction Successful URL
 = tftp://172.19.139.145/audio/ch_welcome.au
172.19.139.145:1057277317:65:INFO: ID = 650922A8: Read request aborted for URL =
tftp://172.19.139.145/audio/ch_welcome.au
-------------------------------------------------------------------------------
Router# show call application interface tftp info

Server name:         172.19.139.145
Statistics:
Last reset time *Jul  3 16:08:13 PST
Read requests:             3
Read successes:            2
Read failures:             0
Read aborts:               1
Total bytes read:               145888
-------------------------------------------------------------------------------
```

The table below describes the significant fields shown in the display.

Table 24: show call application interface Field Descriptions

Field	Description
Last reset time	Time at which the statistics were last cleared with the **clear call application interface** command, or the gateway was restarted.
Read requests	Total number of read requests from applications to this interface type.
Read successes	Number of successful read requests from applications to this interface type.
Read failures	Number of failed read requests from applications to this interface type.
Read aborts	Number of aborted read requests from applications to this interface type.
Total bytes read	Total number of bytes that the application read from this interface type.
Server name	Name of the specific server.
Stats	Whether statistics are enabled for this server.
Error Count	Total number of errors for this server.
Event Log	Whether event logging is enabled for this server.

Related Commands

Command	Description
call application interface event-log	Enables event logging for external interfaces used by voice applications.
call application interface stats	Enables statistics collection for application interfaces.
clear call application interface	Clears application interface statistics and event logs.

show call application services registry

To display a one-line summary of all TCL IVR 2.0 application sessions that have registered as a service, use the **show call application services registry**command in user EXEC or privileged EXEC mode.

show call application services registry

Syntax Description

This command has no arguments or keywords.

Command Default

No default behavior or values

Command Modes

User EXEC (>)
Privileged EXEC (#)

Command History

Release	Modification
12.3(4)T	This command was introduced.

Usage Guidelines

- The services registry is a database that keeps track of every TCL IVR 2.0 application instance that registers as a service. Other TCL applications can then find and communicate with any registered application.
- A TCL session is not registered as a service through a Cisco IOS command. A running instance of a TCL IVR 2.0 application registers itself as a service with the TCL service register command. For information about the service register command, refer to the TCL IVR API Version 2.0 Programmer's Guide.

Examples

The following is sample output for this command:

```
Router# show call application services registry
There are 1 Registered Services
  Service Name          Session ID  Session Name
  data_service                   4  s1
```

The table below describes significant fields in the display.

Table 25: show call application services registry Field Descriptions

Field	Description
Service Name	Name specified by the TCL service register command.
Session ID	ID of the session that registered as this service. You can use this ID in the **show call application sessions id** command to view details about this session.
Session Name	Name configured by the **call application session start** command, if the session was started on the gateway rather than by an incoming call.

Related Commands

Command	Description
call application session start (global configuration)	Starts a new instance (session) of a TCL application from global configuration mode.
call application session start (privileged EXEC)	Starts a new instance (session) of a TCL application from privileged EXEC mode.
call application session stop	Stops a voice application session that is running.
show call application sessions	Displays summary or detailed information about voice application sessions.

show call application session-level

To display event logs and statistics for individual voice application instances, use the **show call application session-level**command in privileged EXEC mode.

show call application {**active** | **history**} **session-level** [**summary** | [**app-tag** *application-name* | **last** [*number*] | **session-id** *session-id*] [**event-log** | **info**]]

Syntax Description

active	Displays event logs or statistics for active application instances.
history	Displays event logs or statistics for inactive application instances in the history table.
summary	Displays a summary of each application instance.
app-tag *application-name*	Name of a specific voice application. Output displays event logs or statistics for that voice application.
last	(Optional) Displays event logs or statistics for the most recent instance.
number	(Optional) Displays event logs or statistics for this number of most recent previous instances.
session-id *session-id*	Identifies a specific application instance. Output displays event logs or statistics for that instance.
event-log	(Optional) Displays event logs for application instances.
info	(Optional) Displays statistics for application instances.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.3(8)T	This command was introduced.

Usage Guidelines

- To display event logs or statistics with this command, you must enable event logging and statistics with the **call application event-log** and **call application stats** command, respectively.
- This command displays gauges and counters that are aggregated per application instance. The values represent an individual instance running on the gateway while statistics collection is enabled.
- The number of records that are included when using the **history** keyword depends on the settings of the **call application history session max-records** and **call application history session retain-timer** commands.

Examples

The following is sample output from the **show call application session-level** command using different keywords and arguments:

```
Router# show call application active session-level summary

SID  Application Name       Stat Err Cnt    Log Start Time
5    generic                Y    6          Y   *Jul  3 15:19:4
6    generic                Y    3          Y   *Jul  3 15:19:5
Router# show call application active session-level last
Session Info:
Session id:          6
Session name:
Application name:    generic
Application URL:     tftp://demo/scripts/primary/generic.vxml
Start time:          *Jul  3 15:19:53 PST
Statistics:
 Subscriber Service - Call
                                                PSTN               VOIP
                                        Incoming Outgoing  Incoming Outgoing
Legs setup:                             1        0         0        0
Total legs connected:                   1        0         0        0
Legs currently connected:               1        0         0        0
Legs handed in:                         0        0         0        0
Legs handed in returned back:           0        0         0        0
Legs handed out:                        0        0         0        0
Legs handed out came back:              0        0         0        0
Legs disconnected normally:             0        0         0        0
Legs disconnected for user error:       0        0         0        0
Legs disconnected for system error:     0        0         0        0
 Subscriber Service - Media
                                        Play       Record     TTS
Media attempts:                         4          0          0
Media actives:                          0          0          0
Media successes:                        0          0          0
Media aborts:                           0          0          0
Media failures:                         4          0          0
Total media duration (in seconds):      0          0          0
 Subscriber Interaction - DTMF
DTMFs not matched:                      0
DTMFs matched:                          0
DTMFs no input:                         3
DTMFs long pound:                       0
Event log:
buf_size=25K, log_lvl=INFO
<ctx_id>:<timestamp>:<seq_no>:<severity>:<msg_body>
6:1057274393:472:INFO: Session started for App-type = generic, URL =
tftp://demo/scripts/primary/generic.vxml
6:1057274393:473:INFO: Incoming Telephony call received, LegID = 10
6:1057274393:474:INFO: LegID = 10: Calling = 4084644753, called = 52927, dial peer = 1
6:1057274393:475:INFO: LegID = 10: Leg State = LEG_INCCONNECTED
6:1057274393:478:INFO: Playing prompt #1: http://172.19.139.145/audio/ch_welcome.au
6:1057274408:517:INFO: Script received event = "error.badfetch"
Router# show call application active session-level info

Session Info:
Session id:          5
Session name:
Application name:    generic
Application URL:     tftp://demo/scripts/primary/generic.vxml
Start time:          *Jul  3 15:19:44 PST
Statistics:
 Subscriber Service - Call
                                                PSTN               VOIP
                                        Incoming Outgoing  Incoming Outgoing
Legs setup:                             1        0         0        0
Total legs connected:                   1        0         0        0
```

```
Legs currently connected:                1        0         0         0
Legs handed in:                          0        0         0         0
Legs handed in returned back:            0        0         0         0
Legs handed out:                         0        0         0         0
Legs handed out came back:               0        0         0         0
Legs disconnected normally:              0        0         0         0
Legs disconnected for user error:        0        0         0         0
Legs disconnected for system error:      0        0         0         0
 Subscriber Service - Media
                                         Play       Record     TTS
Media attempts:                          9          0          0
Media actives:                           0          0          0
Media successes:                         0          0          0
Media aborts:                            0          0          0
Media failures:                          9          0          0
Total media duration (in seconds):       0          0          0
 Subscriber Interaction - DTMF
DTMFs not matched:                       0
DTMFs matched:                           0
DTMFs no input:                          8
DTMFs long pound:                        0
Session Info:
Session id:          6
Session name:
Application name:    generic
Application URL:     tftp://demo/scripts/primary/generic.vxml
Start time:          *Jul  3 15:19:53 PST
Statistics:
 Subscriber Service - Call
                                                PSTN                VOIP
                                         Incoming Outgoing  Incoming Outgoing
Legs setup:                              3        0         0        0
Total legs connected:                    3        0         0        0
Legs currently connected:                1        0         0        0
Legs handed in:                          0        0         0        0
Legs handed in returned back:            0        0         0        0
Legs handed out:                         0        0         0        0
Legs handed out came back:               0        0         0        0
Legs disconnected normally:              0        0         0        0
Legs disconnected for user error:        0        0         0        0
Legs disconnected for system error:      0        0         0        0
 Subscriber Service - Media
                                         Play       Record     TTS
Media attempts:                          7          0          0
Media actives:                           0          0          0
Media successes:                         0          0          0
Media aborts:                            0          0          0
Media failures:                          7          0          0
Media duration (in seconds):             0          0          0
 Application Internal Service - Handoff
                                         Incoming   Outgoing
Bridged handoffs:                        0          0
Bridged handoffs returned:               0          0
Blind handoffs:                          0          0
Handoffs in transit:                     x          0
Handoffs failed:                         x          0
 Application Internal Service - Placecall/transfer
Placecall requests:                      0
Placecall successes:                     0
Placecall failures:                      0
Placecalls in transit:                   0
 Application Internal Service - Document Read-Write
                                         Read       Write
Doc requests:                            0          0
```

```
Doc successes:                          0          0
Doc failures:                           0          0
 Application Internal Service - Downloaded Script
Script parse errors:                    0
 Application Internal Service - ASNL
ASNL notifications:                     0
                                        Subscription   Unsubscription
ASNL requests:                          0              0
ASNL successes:                         0              0
ASNL pendings:                          0              0
ASNL failures:                          0              0
 Subscriber Interaction - DTMF
DTMFs not matched:                      0
DTMFs matched:                          0
DTMFs no input:                         6
DTMFs long pound:                       0
 Subscriber Interaction - ASR
ASRs not matched:                       0
ASRs matched:                           0
ASRs no input:                          0
 Subscriber Interaction - AAA
                                        Authentication Authorization
AAA successes:                          0              0
AAA failures:                           0              0
Router# show call application active session-level event-log

Event log:
buf_size=25K, log_lvl=INFO
<ctx_id>:<timestamp>:<seq_no>:<severity>:<msg_body>
5:1057274384:454:INFO: Session started for App-type = generic, URL =
tftp://demo/scripts/primary/generic.vxml
5:1057274384:455:INFO: Incoming Telephony call received, LegID = D
5:1057274384:456:INFO: LegID = D: Calling = 4085550198, called = 52927, dial peer = 1
5:1057274384:457:INFO: LegID = D: Leg State = LEG_INCCONNECTED
5:1057274384:460:INFO: Playing prompt #1: http://172.19.139.145/audio/ch_welcome.au
5:1057274384:462:ERR : Prompt play setup failure.
5:1057274384:463:INFO: Script received event = "error.badfetch"
5:1057274389:464:INFO: Timed out waiting for user DTMF digits, no user input.
5:1057274389:465:INFO: Script received event = "noinput"
Event log:
buf_size=25K, log_lvl=INFO
<ctx_id>:<timestamp>:<seq_no>:<severity>:<msg_body>
6:1057274393:472:INFO: Session started for App-type = generic, URL =
tftp://demo/scripts/primary/generic.vxml
6:1057274393:473:INFO: Incoming Telephony call received, LegID = 10
6:1057274393:474:INFO: LegID = 10: Calling = 4084644753, called = 52927, dial peer = 1
6:1057274393:475:INFO: LegID = 10: Leg State = LEG_INCCONNECTED
6:1057274393:478:INFO: Playing prompt #1: http://172.19.139.145/audio/ch_welcome.au
6:1057274393:480:ERR : Prompt play setup failure.
6:1057274393:481:INFO: Script received event = "error.badfetch"
6:1057274398:488:INFO: Timed out waiting for user DTMF digits, no user input.
6:1057274398:489:INFO: Script received event = "noinput"
6:1057274398:490:INFO: Playing prompt #1: http://172.19.139.145/audio/ch_welcome.au
Router# show call application active session-level app-tag generic

Session Info:
Session id:          5
Session name:
Application name:    generic
Application URL:     tftp://demo/scripts/primary/generic.vxml
Start time:          *Jul  3 15:19:44 PST
Statistics:
 Subscriber Service - Call
                                                PSTN               VOIP
```

```
                                        Incoming Outgoing  Incoming Outgoing
Legs setup:                             1        0         0        0
Total legs connected:                   1        0         0        0
Legs currently connected:               1        0         0        0
Legs handed in:                         0        0         0        0
Legs handed in returned back:           0        0         0        0
Legs handed out:                        0        0         0        0
Legs handed out came back:              0        0         0        0
Legs disconnected normally:             0        0         0        0
Legs disconnected for user error:       0        0         0        0
Legs disconnected for system error:     0        0         0        0
 Subscriber Service - Media
                                        Play       Record     TTS
Media attempts:                         16         0          0
Media actives:                          0          0          0
Media successes:                        0          0          0
Media aborts:                           0          0          0
Media failures:                         17         0          0
Total media duration (in seconds):      0          0          0
 Subscriber Interaction - DTMF
DTMFs not matched:                      0
DTMFs matched:                          0
DTMFs no input:                         16
DTMFs long pound:                       0
Event log:
buf_size=25K, log_lvl=INFO
<ctx_id>:<timestamp>:<seq_no>:<severity>:<msg_body>
5:1057274384:454:INFO: Session started for App-type = generic, URL =
tftp://demo/scripts/primary/generic.vxml
5:1057274384:455:INFO: Incoming Telephony call received, LegID = D
5:1057274384:456:INFO: LegID = D: Calling = 4085550198, called = 52927, dial peer = 1
5:1057274384:457:INFO: LegID = D: Leg State = LEG_INCCONNECTED
5:1057274384:460:INFO: Playing prompt #1: http://172.19.139.145/audio/ch_welcome.au
5:1057274384:462:ERR : Prompt play setup failure.
5:1057274384:463:INFO: Script received event = "error.badfetch"
5:1057274389:464:INFO: Timed out waiting for user DTMF digits, no user input.
5:1057274389:465:INFO: Script received event = "noinput"
5:1057274389:466:INFO: Playing prompt #1: http://172.19.139.145/audio/ch_welcome.au
Router# show call application active session-level session-id 7
Session Info:
Session id:          7
Session name:
Application name:    generic
Application URL:     tftp://demo/scripts/primary/generic.vxml
Start time:          *Jul  3 15:21:26 PST
Statistics:
 Subscriber Service - Call
                                              PSTN               VOIP
                                        Incoming Outgoing  Incoming Outgoing
Legs setup:                             1        0         0        0
Total legs connected:                   1        0         0        0
Legs currently connected:               1        0         0        0
Legs handed in:                         0        0         0        0
Legs handed in returned back:           0        0         0        0
Legs handed out:                        0        0         0        0
Legs handed out came back:              0        0         0        0
Legs disconnected normally:             0        0         0        0
Legs disconnected for user error:       0        0         0        0
Legs disconnected for system error:     0        0         0        0
 Subscriber Service - Media
                                        Play       Record     TTS
Media attempts:                         3          0          0
Media actives:                          0          0          0
Media successes:                        0          0          0
```

```
Media aborts:                              0          0          0
Media failures:                            3          0          0
Total media duration (in seconds):         0          0          0
 Subscriber Interaction - DTMF
DTMFs not matched:                         0
DTMFs matched:                             0
DTMFs no input:                            2
DTMFs long pound:                          0
Event log:
buf_size=25K, log_lvl=INFO
<ctx_id>:<timestamp>:<seq_no>:<severity>:<msg_body>
7:1057274486:662:INFO: Session started for App-type = generic, URL =
tftp://demo/scripts/primary/generic.vxml
7:1057274486:663:INFO: Incoming Telephony call received, LegID = 13
7:1057274486:664:INFO: LegID = 13: Calling = 4085550198, called = 52927, dial peer = 1
7:1057274486:665:INFO: LegID = 13: Leg State = LEG_INCCONNECTED
7:1057274486:668:INFO: Playing prompt #1: http://172.19.139.145/audio/ch_welcome.au
Router# show call application history session-level summary

SID  Application Name       Stat Err Cnt    Log Stop Time       Duration
1    generic                Y    3          Y   *Jul  3 15:49:2 00:00:11
2    generic                Y    1          Y   *Jul  3 15:49:3 00:00:03
Router# show call application history session-level last

Session Info:
Session id:          2
Session name:
Application name:    generic
Application URL:     tftp://demo/scripts/primary/generic.vxml
Start time:          *Jul  3 15:49:29 PST
Stop time:           *Jul  3 15:49:33 PST
Statistics:
 Subscriber Service - Call
                                                  PSTN                VOIP
                                           Incoming Outgoing  Incoming Outgoing
Legs setup:                                1        0         0        0
Total legs connected:                      1        0         0        0
Legs handed in:                            0        0         0        0
Legs handed in returned back:              0        0         0        0
Legs handed out:                           0        0         0        0
Legs handed out came back:                 0        0         0        0
Legs disconnected normally:                1        0         0        0
Legs disconnected for user error:          0        0         0        0
Legs disconnected for system error:        0        0         0        0
 Subscriber Service - Media
                                           Play       Record     TTS
Media attempts:                            1          0          0
Media successes:                           0          0          0
Media aborts:                              0          0          0
Media failures:                            1          0          0
Total media duration (in seconds):         0          0          0
Event log:
buf_size=25K, log_lvl=INFO
<ctx_id>:<timestamp>:<seq_no>:<severity>:<msg_body>
2:1057276169:28:INFO: Session started for App-type = generic, URL =
tftp://demo/scripts/primary/generic.vxml
2:1057276169:29:INFO: Incoming Telephony call received, LegID = 4
2:1057276169:30:INFO: LegID = 4: Calling = 4085550198, called = 52927, dial peer = 1
2:1057276169:31:INFO: LegID = 4: Leg State = LEG_INCCONNECTED
2:1057276169:34:INFO: Playing prompt #1: http://172.19.139.145/audio/ch_welcome.au
2:1057276169:36:ERR : Prompt play setup failure.
2:1057276169:37:INFO: Script received event = "error.badfetch"
2:1057276173:39:INFO: Script received event = "telephone.disconnect.hangup"
2:1057276173:40:INFO: LegID = 4: Call disconnected, cause = normal call clearing (16)
```

```
2:1057276173:43:INFO: Session done, terminating cause =
Router# show call application history session-level event-log

Event log:
buf_size=25K, log_lvl=INFO
<ctx_id>:<timestamp>:<seq_no>:<severity>:<msg_body>
1:1057276157:3:INFO: Session started for App-type = generic, URL =
tftp://demo/scripts/primary/generic.vxml
1:1057276157:4:INFO: Incoming Telephony call received, LegID = 1
1:1057276157:5:INFO: LegID = 1: Calling = 4085550198, called = 52927, dial peer = 1
1:1057276157:6:INFO: LegID = 1: Leg State = LEG_INCCONNECTED
1:1057276157:9:INFO: Playing prompt #1: http://172.19.139.145/audio/ch_welcome.au
1:1057276160:12:ERR : Prompt play setup failure.
1:1057276160:13:INFO: Script received event = "error.badfetch"
1:1057276165:14:INFO: Timed out waiting for user DTMF digits, no user input.
1:1057276165:15:INFO: Script received event = "noinput"
1:1057276165:16:INFO: Playing prompt #1: http://172.19.139.145/audio/ch_welcome.au
1:1057276165:18:ERR : Prompt play setup failure.
1:1057276165:19:INFO: Script received event = "error.badfetch"
1:1057276168:21:INFO: Script received event = "telephone.disconnect.hangup"
1:1057276168:22:INFO: LegID = 1: Call disconnected, cause = normal call clearing (16)
1:1057276168:25:INFO: Session done, terminating cause =
Event log:
buf_size=25K, log_lvl=INFO
<ctx_id>:<timestamp>:<seq_no>:<severity>:<msg_body>
2:1057276169:28:INFO: Session started for App-type = generic, URL =
tftp://demo/scripts/primary/generic.vxml
2:1057276169:29:INFO: Incoming Telephony call received, LegID = 4
2:1057276169:30:INFO: LegID = 4: Calling = 4085550198, called = 52927, dial peer = 1
2:1057276169:31:INFO: LegID = 4: Leg State = LEG_INCCONNECTED
2:1057276169:34:INFO: Playing prompt #1: http://172.19.139.145/audio/ch_welcome.au
2:1057276169:36:ERR : Prompt play setup failure.
2:1057276169:37:INFO: Script received event = "error.badfetch"
2:1057276173:39:INFO: Script received event = "telephone.disconnect.hangup"
2:1057276173:40:INFO: LegID = 4: Call disconnected, cause = normal call clearing (16)
2:1057276173:43:INFO: Session done, terminating cause =
Router# show call application history session-level info

Session Info:
Session id:          1
Session name:
Application name:    generic
Application URL:     tftp://demo/scripts/primary/generic.vxml
Start time:          *Jul  3 15:49:17 PST
Stop time:           *Jul  3 15:49:28 PST
Statistics:
 Subscriber Service - Call
                                                PSTN              VOIP
                                       Incoming Outgoing  Incoming Outgoing
Legs setup:                            1        0         0        0
Total legs connected:                  1        0         0        0
Legs handed in:                        0        0         0        0
Legs handed in returned back:          0        0         0        0
Legs handed out:                       0        0         0        0
Legs handed out came back:             0        0         0        0
Legs disconnected normally:            1        0         0        0
Legs disconnected for user error:      0        0         0        0
Legs disconnected for system error:    0        0         0        0
 Subscriber Service - Media
                                       Play       Record     TTS
Media attempts:                        2          0          0
Media successes:                       0          0          0
Media aborts:                          0          0          0
Media failures:                        2          0          0
```

```
Total media duration (in seconds):         3          0          0
 Subscriber Interaction - DTMF
DTMFs not matched:                         0
DTMFs matched:                             0
DTMFs no input:                            1
DTMFs long pound:                          0
Session Info:
Session id:          2
Session name:
Application name:    generic
Application URL:     tftp://demo/scripts/primary/generic.vxml
Start time:          *Jul  3 15:49:29 PST
Stop time:           *Jul  3 15:49:33 PST
Statistics:
 Subscriber Service - Call
                                                  PSTN                VOIP
                                           Incoming Outgoing  Incoming Outgoing
Legs setup:                                1        0         0        0
Total legs connected:                      1        0         0        0
Legs handed in:                            0        0         0        0
Legs handed in returned back:              0        0         0        0
Legs handed out:                           0        0         0        0
Legs handed out came back:                 0        0         0        0
Legs disconnected normally:                1        0         0        0
Legs disconnected for user error:          0        0         0        0
Legs disconnected for system error:        0        0         0        0
 Subscriber Service - Media
                                           Play       Record     TTS
Media attempts:                            1          0          0
Media successes:                           0          0          0
Media aborts:                              0          0          0
Media failures:                            1          0          0
Total media duration (in seconds):         0          0          0
```

The table below describes significant fields in the displays.

Note These fields display for the **show call application session-level**, **show call application app-level**, and **show call application gateway-level** commands. At the session level, the fields apply to a single application instance. At the application level, the fields apply to all instances of an application. At the gateway level, the fields apply to all instances of all applications.

Table 26: show call application active session-level info Field Descriptions

Field	Description
Session id	Session ID assigned to the instance when it became active.
Session name	Name of the session defined with the **call application session start** command.
Application name	Name of the application defined with the **call application voice** command.
Application URL	Location of the application script defined with the **call application voice** command.
Start time	Time at which the session started.

Field	Description
Subscriber Service -- Call	
Legs setup	Number of calls setup (indications and requests) by an application instance.
Total legs connected	Number of calls connected by an application instance.
Legs currently connected	Number of calls currently connected by an application instance at any moment.
Legs handed in	Number of call legs received as an incoming handoff from another application.
Legs handed in returned back	Number of call legs received as an incoming handoff from another application that were returned to the other application.
Legs handed out	Number of call legs handed off to another application.
Legs handed out came back	Number of call legs handed off to another application that were returned by the other application.
Legs disconnected normally	Number of incoming and outgoing calls disconnected for normal causes.
Legs disconnected for user error	Number of incoming calls disconnected for call failure reasons, such as no answer or busy.
Legs disconnected for system error	Number of incoming calls disconnected for system failure reasons, such as no resources.
Subscriber Service -- Media	
Media attempts	Number of prompt playouts, recordings, and text-to-speech (TTS) attempts on call legs in this application instance.
Media actives,	Number of prompt playouts, recordings, and TTS prompts currently active on call legs in an application instance.
Media successes	Number of prompt playouts, recordings, and TTS prompts that were successful on call legs in an application instance.
Media aborts	Number of prompt playouts, recordings, and TTS prompts that were aborted by the caller on call legs in an application instance.
Media failures	Number of prompt playouts, recording, and TTS attempts that failed on call legs in an application instance.
Total media duration	Total duration, in seconds, of prompt playing, recording, or TTS.
Application Internal Service -- Handoff	
Bridged handoffs, incoming	Number of handoffs received with callback (bridged transfers) in an application instance.

Field	Description
Bridged handoffs, outgoing	Number of handoffs placed with callback (bridged transfers) by an application instance.
Bridged handoffs returned, incoming	Number of incoming bridged handoffs that were returned by an application instance.
Bridged handoffs returned, outgoing	Number of outgoing bridged handoffs that were returned to an application instance.
Blind handoffs, incoming	Number of handoffs received with no callback (blind transfers) in an application instance.
Blind handoffs, outgoing	Number of handoffs placed with no callback (blind transfers) by an application instance.
Handoffs in transit[1]	Number of handoffs in progress for an application instance. The value is decremented by one after the receiving application either hands back the application or rejects the handoff.
Handoffs failed	Number of handoffs that failed (bridged and blind) in an application instance.
Application Internal Service -- Placecall/transfer	
Placecall requests	Number of outgoing call setup requests made by an application instance.
Placecall successes	Number of outgoing calls placed by an application instance.
Placecall failures	Number of outgoing call setup requests that failed for an application instance.
Place calls in transit	Number of outgoing calls in progress for an application. The value is decremented by one after the call is either set up or the setup fails.
Application Internal Service -- Document Read-Write	
Doc requests	Number of document fetch and submit requests.
Doc successes	Number of successful document fetches and submits.
Doc failures	Number of document fetch and submit failures.
Application Internal Service -- Downloaded Script	
Script parse errors	Number of semantic errors seen by an application instance.
Application Internal Service -- ASNL	

Field	Description
ASNL notifications	Number of Application Subscribe Notify Layer (ASNL) notifications received from servers.
ASNL requests	Number of subscribe or unsubscribe requests made by an application instance.
ASNL successes	Number of subscribe or unsubscribe requests that succeeded for an application instance.
ANSL failures	Number of subscribe or unsubscribe requests that failed for an application instance.
Subscriber Interaction --- DTMF	
DTMFs not matched	Number of DTMF patterns input by a caller that were not matched in an application instance.
DTMFs matched	Number of DTMF patterns input by a caller that were matched in an application instance.
DTMFs no input	Number of "no input" notifications received (includes DTMF timeouts).
DTMFs long pound	Number of long-pound interrupts from a caller seen by an application instance.
Subscriber Interaction -- ASR	
ASR not matched	Number of automatic speech recognition (ASR) phrases from a caller that were not matched in an application instance.
ASR matched	Number of automatic speech recognition (ASR) phrases from a caller that were matched in an application instance.
ASR no inputs	Number of "no input" notifications received from ASR servers.
Subscriber Interaction -- AAA Authentication	
AAA authentication successes	Number of AAA authentication successes.
AAA authentication failures	Number of AAA authentication failures because of invalid passwords.
Subscriber Interaction -- AAA Authorizations	
AAA authorization successes	Number of AAA authorization successes.
AAA authorization failures	Number of AAA authorization failures.

[1] When this gauge is greater than zero, the application instance might stop processing the script and the counters and gauges may appear to freeze. When the handoff or the placecall operation

is finished and control is returned to the application instance, the counters and gauges are updated.

Related Commands

Command	Description
call application event-log	Enables event logging for voice application instances.
call application history session max-records	Sets the maximum number of application instance records saved in history.
call application history session retain-timer	Sets the maximum number of minutes for which application instance records are saved in history.
call application stats	Enables statistics collection for voice applications.
call application voice event-log	Enables event logging for a specific voice application.
show call application app-level	Displays application-level statistics for voice applications.
show call application gateway-level	Displays gateway-level statistics for voice application instances.

show call application sessions

To display summary or detailed information about all running or stopped voice application sessions, use the **show call application sessions** command in user EXEC or privileged EXEC mode.

show call application sessions [**callid** *call-id* | **id** *session-id* | **name** *instance-name*]

Syntax Description

callid *call-id*	(Optional) Call-leg ID of an active call that is being controlled by the session.
id *session-id*	(Optional) Session ID for the specific application instance.
name *instance-name*	(Optional) Name assigned to the instance with the **call application session start** command.

Command Default

No default behavior or values

Command Modes

User EXEC (>)
Privileged EXEC (#)

Command History

Release	Modification
12.3(4)T	This command was introduced.

Usage Guidelines

- A specific application session is identified by one of three different methods: call ID, session ID, or instance name.
- If a specific session is identified by a **callid**, **id**, or **name** keyword, this command displays information about that specific session only. If you do not use a keyword, this command displays a one-line summary of all sessions, not just those sessions that are started by the **call application session start** command.
- This command lists all running TCL IVR 2.0 and VoiceXML application sessions and TCL sessions that are stopped. A session displays a state of "stopped" if you intentionally stop it with the **call application session stop** or **no call application session start** command, or because there is a syntax error that prevents the script from running. This is the case only if the session is started with the **call application session start** command through global configuration mode.

Note If a session is started with the **call application session start** command in privileged EXEC mode, it is not tracked by the system and is therefore not shown as stopped in the output of the **show call application sessions** command.

Examples

The following is sample output from this command:

```
Router# show call application sessions
TCL Sessions
    There are 1 active TCL sessions
```

```
     SID  Name        Called     Calling               App Name               Legs
       5  serv1                                        sample_service
VXML Sessions
    No running VXML sessions
Stopped Sessions
  Instance Name        App Name             State
  my_instance1         sample               stopped
```

The table below describes significant fields in the display.

Table 27: show call application sessions Field Descriptions

Field	Description
SID	Session identifier for active sessions.
Name	Session name that was configured with the **call application session start** command.
Called	Called number for active calls that are using the session.
Calling	Calling number for active calls that are using the session.
App Name	Name of the application for which the instance was created.
Legs	Any active call legs that are controlled by the session.
State	Shows "stopped" for any session that is no longer running, provided that the session is started with the **call application session start** command in global configuration mode.

The following is sample output for a session named serv1:

```
Router# show call aplication sessions name serv1
Session named serv1 is in the start list in state running
  It is configured to start on GW reboot
  The application it runs is sample_service
  Handle is TCL_HAND*1653710732*0*3193204
TCL Session ID B
                App: sample_service
                URL: tftp://dev/demo/scripts/sample_service.tcl
       Session name: serv1
     Session handle: TCL_HAND*1653710732*0*3193204
          FSM State: start_state
   ID for 'show call active voice id' display: 0
               Legs:
           Services: data_service
```

The table below describes significant fields in the display.

Table 28: show call application sessions name Field Descriptions

Field	Description
App	Name of the application for which the instance was created.
URL	Location of the script used for the application as specified with the **call application voice** command.
Session name	Session name that was configured with the **call application session start** command.

Field	Description
Session handle	Handle that is returned from the TCL mod_handle infotag. A session handle is used in a TCL script on a Cisco gateway to send messages to other sessions.
FSM State	Current state in the TCL IVR 2.0 finite-state machine, as specified with the TCL fsm setstate command in the script.
ID for 'show call active voice id' display:	Call identifier.
Legs	Any active call legs that are controlled by this session.
Services	Service name for the session if it registered as a service with the TCL service register command in the script. You can display a list of all registered services with the **show call application services registry** command.

Related Commands

Command	Description
call application session start (global configuration)	Starts a new instance (session) of a TCL application from global configuration mode.
call application session start (privileged EXEC)	Starts a new instance of a TCL application from privileged EXEC mode.
call application session stop	Stops a voice application session that is running.
show call application services registry	Displays a one-line summary of all registered services.

show call application voice

To display information about voice applications, use the **show call application voice** command in EXEC mode.

show call application voice [*name* | **summary**]

Syntax Description

name	(Optional) Name of the desired voice application. Output displays information about that application.
summary	(Optional) Output displays a one-line summary of each voice application.

Command Default

If both the *name* argument and **summary** keyword are omitted, command output displays detailed information about all interactive voice response (IVR) applications.

Command Modes

EXEC (#)

Command History

Release	Modification
11.3(6)NA2	This command was introduced.
12.0(3)T	This command was integrated into Cisco IOS Release 12.0(3)T.
12.1(5)T	This command was implemented on the Cisco AS5800.
12.1(5)XM2	This command was implemented on the Cisco AS5350 and Cisco AS5400.
12.2(2)XB	This command was modified to support VoiceXML applications.
12.2(2)XB1	This command was implemented on the Cisco AS5850.
12.2(4)XM	This command was implemented on the Cisco 1750 and Cisco 1751. This command was not supported on any other platforms in this release.
12.2(8)T	This command was implemented on the Cisco 1751, Cisco 2600 series, Cisco 3600 series, Cisco 3725, Cisco 3745, and Cisco 7200.
12.2(11)T	This command was integrated into Cisco IOS Release 12.2(11)T for VoiceXML applications. This command is supported on the Cisco AS5300, Cisco AS5350, Cisco AS5400, and Cisco AS5850 in this release.
12.3(14)T	New output was added relating to the SCCP Telephony Control Application (STCAPP).

Usage Guidelines

The **show call application voice**command displays a detailed description of each configured application.

If the name of a specific application is entered, the command displays detailed information about only that application.

If the **summary** keyword is entered, the command displays a one-line summary about each application.

If STCAPP is enabled, the **summary** command displays STCAPP as an available call application.

If an asterisk is displayed next to the application name when the **summary** keyword is used, the application is configured, but not running. Normally this is because the application was not successfully loaded, for example:

```
name                description
*vapptest2          flash:helloworld.vxml
```

TCL scripts and VoiceXML documents can be stored in any of the following locations: TFTP, FTP, or HTTP servers; Flash memory of the gateway; or the removable disks of the Cisco 3600 series. The audio files that they use can be stored in any of these locations and on RTSP servers.

Examples

The following example shows the output for the session Toolkit Command Language (TCL) script:

```
Router# show call application voice session
Application session
    The script is compiled into the image
    It has 0 calls active.
    Interpreted by infrastructure version 2.0
The TCL Script is:
-----------------
# app_session.tcl
#---------------------------------
# August 1999, Saravanan Shanmugham
#
# Copyright (c) 1998, 1999, 2000, 2001 by cisco Systems, Inc.
# All rights reserved.
#---------------------------------
#
# This tcl script mimics the default SESSION app
#
# If DID is configured, just place the call to the dnis
# Otherwise, output dial-tone and collect digits from the
# caller against the dial-plan.
#
# Then place the call. If successful, connect it up, otherwise
# the caller should hear a busy or congested signal.
# The main routine just establishes the statemachine and then exits.
# From then on the system drives the statemachine depending on the
# events it recieves and calls the appropriate tcl procedure
#---------------------------------
#   Example Script
#---------------------------------
proc init { } {
    global param
    set param(interruptPrompt) true
    set param(abortKey) *
    set param(terminationKey) #
}
proc act_Setup { } {
    global dest
    global beep
    set beep 0
    if { [infotag get leg_isdid] } {
        set dest [infotag get leg_dnis]
        leg proceeding leg_incoming
        leg setup $dest callInfo leg_incoming
        fsm setstate PLACECALL
    } else {
        leg setupack leg_incoming
        playtone leg_incoming tn_dial
        set param(dialPlan) true
```

```
        leg collectdigits leg_incoming param
    }
}
proc act_GotDest { } {
    global dest
    set status [infotag get evt_status]
    if {  $status == "cd_004" } {
        set dest [infotag get evt_dcdigits]
        leg proceeding leg_incoming
        leg setup $dest callInfo leg_incoming
    } else {
        puts "\nCall [infotag get con_all] got event $status collecting destina"
        call close
    }
}
proc act_CallSetupDone { } {
    global beep
    set status [infotag get evt_status]
    if { $status == "ls_000"} {
        set  creditTimeLeft [infotag get leg_settlement_time leg_all]
        if { ($creditTimeLeft == "unlimited") ||
             ($creditTimeLeft == "uninitialized") } {
            puts "\n Unlimited Time"
        } else {
            # start the timer for ...
            if { $creditTimeLeft < 10 } {
                set beep 1
                set delay $creditTimeLeft
            } else {
                set delay [expr $creditTimeLeft - 10]
            }
            timer start leg_timer $delay leg_incoming
        }
    } else {
        puts "Call [infotag get con_all] got event $status collecting destinati"
        call close
    }
}
proc act_Timer { } {
    global beep
    global incoming
    global outgoing
    set incoming [infotag get leg_incoming]
    set outgoing [infotag get leg_outgoing]
    if { $beep == 0 } {
        #insert a beep ...to the caller
        connection destroy con_all
        set beep 1
    } else {
        connection destroy con_all
        fsm setstate LASTWARN
    }
}
proc act_LastWarn { } {
    media play leg_incoming flash:out_of_time.au
}
proc act_Destroy { } {
    media play leg_incoming flash:beep.au
}
proc act_Beeped { } {
    global incoming
    global outgoing
    connection create $incoming $outgoing
}
```

```
proc act_ConnectedAgain { } {
    timer start leg_timer 10 leg_incoming
}
proc act_Ignore { } {
# Dummy
    puts "Event Capture"
}
proc act_Cleanup { } {
    call close
}
init
#----------------------------------
#   State Machine
#------------------
  set fsm(any_state,ev_disconnected)  "act_Cleanup              same_state"
  set fsm(CALL_INIT,ev_setup_indication) "act_Setup            GETDEST"
  set fsm(GETDEST,ev_collectdigits_done)  "act_GotDest          PLACECALL"
  set fsm(PLACECALL,ev_setup_done)    "act_CallSetupDone    CALLACTIVE"
  set fsm(CALLACTIVE,ev_leg_timer)    "act_Timer            INSERTBEEP"
  set fsm(INSERTBEEP,ev_destroy_done) "act_Destroy          same_state"
  set fsm(INSERTBEEP,ev_media_done)   "act_Beeped           same_state"
  set fsm(INSERTBEEP,ev_create_done)    "act_ConnectedAgain   CALLACTIVE"
  set fsm(LASTWARN,ev_destroy_done)     "act_LastWarn        CALLDISCONNECT"
  set fsm(CALLACTIVE,ev_disconnected)   "act_Cleanup         CALLDISCONNECT"
  set fsm(CALLDISCONNECT,ev_disconnected)   "act_Cleanup         same_state"
  set fsm(CALLDISCONNECT,ev_media_done)     "act_Cleanup         same_state"
  set fsm(CALLDISCONNECT,ev_disconnect_done) "act_Cleanup         same_state"
  set fsm(CALLDISCONNECT,ev_leg_timer)      "act_Cleanup         same_state"
  fsm define fsm CALL_INIT
```

The following is sample output for the **summary** keyword:

```
Router# show call application voice summary
name                 description
session              Basic app to do DID, or supply dialtone.
fax_hop_on           Script to talk to a fax redialer
clid_authen          Authenticate with (ani, dnis)
clid_authen_collect  Authenticate with (ani, dnis), collect if that fails
clid_authen_npw      Authenticate with (ani, NULL)
clid_authen_col_npw  Authenticate with (ani, NULL), collect if that fails
clid_col_npw_3       Authenticate with (ani, NULL), and 3 tries collecting
clid_col_npw_npw     Authenticate with (ani, NULL) and 3 tries without pw
DEFAULT              Default system session application
lib_off_app          Libretto Offramp
TCL Script Version 2.0 supported.
TCL Script Version 1.1 supported.
Voice Browser Version 2.0 for VoiceXML 1.0 & 2.0 supported.
```

The following is sample output for the **summary** keyword when STCAPP is enabled:

```
Router# show call application voice summary

 SERVICES (standalone applications):
  name                      type            description
  ipsla-responder           Tcl Script      builtin:app_test_rcvr_script.tcl
  clid_authen               Tcl Script      builtin:app_clid_authen_script.tcl
  clid_col_npw_npw          Tcl Script      builtin:app_clid_col_npw_npw_script.tcl
  DEFAULT                   C Script        builtin:Session_Service.C
  CTAPP                     C Script        builtin:CallTreatment_Service.C
  clid_authen_col_npw       Tcl Script      builtin:app_clid_authen_col_npw_script.tcl
  fax_hop_on                Tcl Script      builtin:app_fax_hop_on_script.tcl
  ipsla-testcall            Tcl Script      builtin:app_test_place_script.tcl
  clid_authen_npw           Tcl Script      builtin:app_clid_authen_npw_script.tcl
```

```
  session                   Tcl Script      builtin:app_session_script.tcl
  clid_authen_collect       Tcl Script      builtin:app_clid_authen_collect_script.tcl
  clid_col_npw_3            Tcl Script      builtin:app_clid_col_npw_3_script.tcl
  lib_off_app               CCAPI           Libretto Offramp
  DEFAULT.C.OLD             CCAPI           Obsolete system session application
  stcapp                    CCAPI           SCCP Call Control Application
  MGCPAPP                   CCAPI           MGCP Application
```

The following is sample output for the *stcapp* keyword when the STCAPP is enabled:

```
Router# show call application voice stcapp

App Status:              Active
CCM Status:              UP
CCM Group:               2
Registration Mode:       CCM
Total Devices:           5
Total Calls in Progress: 0
Total Call Legs in Use:  0
```

The following is sample output from the show call application voice command for a VoiceXML application named vapptest1:

```
Router# show call application voice vapptest1
VXML Application vapptest1
    URL=flash:demo0.vxml
    Security not trusted
    No languages configured
    It has: 0 calls active.
          0 incoming calls
          0 calls handed off to it
          0 call transfers initiated
          0 pages loaded,  0 successful
          0 prompts played
          0 recorded messages
    Interpreted by Voice Browser Version 2.0 for VoiceXML 1.0 & 2.0.
The VXML Script is:
------------------
<?xml version="1.0"?>
<vxml version="1.0">
  <form>
     <block>
      <audio src="flash:demo0.au"/>
    </block>
  </form>
</vxml>
```

The table below describes the fields shown in the **show call application voice** display:

Table 29: show call application voice Field Descriptions

Field	Description
URL	Location of the document used by the application.
It has: *n* calls active.	Number of calls that are using this application.
incoming calls	Number of incoming public switched telephone network (PSTN) or IP calls that invoked this application.

Field	Description
calls handed off to it	Number of calls that were handed off to this application by another TCL or VoiceXML application.
call transfers initiated	Number of call transfers that were initiated by this application.
pages loaded	Number of VoiceXML pages that were loaded by the application.
successful	Number of VoiceXML pages that were completed.
prompts played	Number of audio prompts that were played by the application.
recorded messages	Number of audio recordings made by the VoiceXML application.
Interpreted by	Programming language used by the application.
The TCL or VoiceXML Script is	Content of the VoiceXML document or TCL script.

Related Commands

Command	Description
call application voice	Defines the name to be used for an application and indicates the location of the appropriate IVR script to be used with the application.
call application voice load	Reloads the designated TCL script or VoiceXML document.

show call fallback cache

To display the current Calculated Planning Impairment Factor (ICPIF) estimates for all IP addresses in cache, use the **show call fallback cache** command in EXEC mode.

show call fallback cache [*ip-address*]

Syntax Description

ip -address	(Optional) Specific IP address.

Command Modes

EXEC (#)

Command History

Release	Modification
12.1(3)T	This command was introduced on the Cisco 2600 series, Cisco 3600 series, and Cisco MC3810.
12.2(2)XB1	This command was implemented on the Cisco AS5850.
12.2(11)T	This command was integrated into Cisco IOS Release 12.2(11)T.

Usage Guidelines

Use this command to clear all entries in the cache.

Examples

The following example displays output from this command:

```
Router# show call fallback cache
Probe   IP Address      Codec   Delay   Loss    ICPIF   Reject  Accept
-----   ----------      -----   -----   ----    -----   ------  ------
1       1.1.1.4         g729r8  40      0     0       0       9
2       122.24.56.25    g729r8  148     10      5       1       4
2 active probes
Field                      Description
-------                    ------------
Probe                      Probe number
IP Address                 IP Address to which the probe is sent
Codec                      Codec Type of the probe
Delay                      Delay in milliseconds that the probe incurred
Loss                       Loss in % that the probe incurred
ICPIF                      Computed ICPIF value for the probe
Reject                     Number of times that calls of Codec Type <Codec>
                           were rejected to the IP Address
Accept                     Number of times that calls of Codec Type <Codec>
                           were accepted to the IP Address
active probes              Number of destinations being probed
Router# show call fallback cache 10.14.115.53
Probe   IP Address      Codec           ICPIF   Reject  Accept
-----   ----------      -----           -----   ------  ------
1       10.14.115.53     g729r8          0       0       2
1 active probes
```

Field descriptions should be self-explanatory.

Related Commands

Command	Description
show call fallback stats	Displays call fallback statistics.

show call fallback config

To display the call fallback configuration, use the **show call fallback config** command in EXEC mode.

show call fallback config

Syntax Description

This command has no arguments or keywords.

Command Modes

EXEC (#)

Command History

Release	Modification
12.1(3)T	This command was introduced on the Cisco 2600 series, Cisco 3600 series, and Cisco MC3810.
12.2(2)XB1	This command was implemented on the Cisco AS5850.
12.2(11)T	This command was integrated into Cisco IOS Release 12.2(11)T.

Examples

The following example displays output from the **show call fallback config** command:

```
Router# show call fallback config
VoIP fallback config:
Fallback is ON
Using ICPIF threshold:
        ICPIF value timeout:20 seconds
        ICPIF threshold:20
Number of packets in a probe:20
IP precedence of probe packets:2
Fallback cache size:2 entries
Fallback cache timeout:240 seconds
Instantaneous value weight:65
MD5 Keychain:secret
```

The table below describes the fields shown in the **show call fallback config** display.

Table 30: show call fallback config Field Descriptions

Field	Description
Fallback is	Lists enabled/disabled state of call fallback.
Using ICPIF threshold	ICPIF is configured to determine network traffic.
ICPIF value timeout	Lists probe timeout for collecting ICPIF information.
ICPIF threshold	Lists configured ICPIF threshold.
Number of packets in a probe	Lists number of configured packets per probe.
IP precedence of probe packets	Lists configured IP precedence for probes.
Fallback cache size	Number of allowed entries in call fallback cache.

Field	Description
Fallback cache timeout	Length of cache timeout, in seconds.
Instantaneous value weight	Lists weight configured for calculating cache entry based on new probe and last entry.
MD5 Keychain	MD5 authentication has been configured with a keychain of secret.

Related Commands

Command	Description
call fallback monitor	Enables the monitoring of destinations without fallback to alternate dial peers.
show voice trunk-conditioning signaling	Enables fallback to alternate dial peers in case of network congestion.

show call fallback stats

To display the call fallback statistics, use the **show call fallback stats** command in EXEC mode.

show call fallback stats

Syntax Description

This command has no arguments or keywords.

Command Modes

EXEC (#)

Command History

Release	Modification
12.1(3)T	This command was introduced on the Cisco 2600, Cisco 3600, and Cisco MC3810.
12.2(2)XB1	This command was implemented on the Cisco AS5850.
12.2(11)T	This command was integrated into Cisco IOS Release 12.2(11)T.

Usage Guidelines

To remove all values, use the **clear call fallback stats** command.

Examples

The following example displays output from the **show call fallback stats** command:

```
Router# show call fallback stats
VOIP Fallback Stats:
Total accepted calls:3
Total rejected calls:1
Total cache overflows:1
Field                       Description
-------                     ------------
Total accepted calls        Number of times that calls were successful over IP.
Total rejected calls        Number of times that calls were rejected over IP.
Total cache overflows       Number of times that the fallback cache overflowed and required
 pruning.
The table below describes the fields shown in the show call fallback stats
display
```

Table 31: show call fallback stats Fields with Descriptions

Field	Description
Total accepted calls	Number of times that calls were successful over IP.
Total rejected calls	Number of times that calls were rejected over IP.
Total cache overflows	Number of times that the fallback cache overflowed and required pruning.

Related Commands

Command	Description
clear call fallback stats	Clears the call fallback statistics.

Command	Description
show call fallback cache	Displays the current ICPIF estimates for all IP addresses in the cache.

show call filter components

To display the components used for filtering calls, use the show call filter components command in privileged EXEC mode.

show call filter components

Command Default

No default behavior or values

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.3(4)T	This command was introduced.
Cisco IOS XE Release 3.10S	This command was integrated into Cisco IOS XE Release 3.10S.

Examples

The following example shows the output from running the show call filter components command. The GCFM is the generic call filter module, which is the internal module that controls which components are filtered:

```
Router# show call filter components
 The following components registered in GCFM:
     ISDN
     VTSP
     CCAPI
     TGRM
     DIAL-PEER
     NUMBER-TRANSLATION
     SSAPP
     VOICE-IVR-V2
     H323
     SIP
     CRM
     TSP
     FAX-FOIP
     FAX-FMSP
     FAX-DMSP
     FAX-MSPI
     FAX-MTA
     DSPAPI
     MGCP
     DSMP
     H221
```

The table below describes the significant fields shown in the display.

Table 32: show call filter components Field Descriptions

Field	Description
The following components registered in GCFM:	Shows which components are filtered in the generic call filter module.

Related Commands

Command	Description
call filter match-list voice	Create a call filter match list for debugging voice calls.
debug call filter inout	Display the debug trace inside the GCFM.
debug condition match-list	Run a filtered debug on a voice call.
outgoing port	Configure debug filtering for the outgoing port.
show call filter match-list	Display call filter match lists.

show call filter match-list

To display call filter match lists, use the show call filter match-list command in privileged EXEC mode.

show call filter match-list *tag*

Syntax Description

tag	Numeric label that uniquely identifies the match list.

Command Default

No default behavior or values.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.3(4)T	This command was introduced.
Cisco IOS XE Release 3.10S	This command was integrated into Cisco IOS XE Release 3.10S.

Examples

The following example shows an output from the show call filter match-list command:

```
Router# show call filter match-list


*****************************************
call filter match-list 9 voice
*****************************************
  incoming calling-number 50200
  incoming called-number 50201
  incoming signal local ipv4 10.0.101.22
  incoming signal remote ipv4  10.0.101.21
  incoming media local ipv4  10.0.101.22
  incoming media remote ipv4  10.0.101.21
  incoming dialpeer 502
  outgoing calling-number 50200
  outgoing called-number 50201
  outgoing port 6/0:D
  outgoing dialpeer 501
 debug condition match-list is set to EXACT_MATCH
*****************************************
call filter match-list 10 voice
*****************************************
  incoming calling-number 50300
  incoming called-number 50301
  incoming signal local ipv4 10.0.101.22
  incoming signal remote ipv4  10.0.101.21
  incoming media local ipv4  10.0.101.22
  incoming media remote ipv4  10.0.101.21
  incoming dialpeer 504
  outgoing calling-number 50300
  outgoing called-number 50301
  outgoing port 6/1:D
  outgoing dialpeer 503
 debug condition match-list is set to EXACT_MATCH
```

The table below describes the significant fields shown in the display.

Table 33: show call filter match-list Field Descriptions

Field	Description
call filter match-list 9 voice	Shows which match list is being displayed.
debug condition match-list is set to EXACT_MATCH	Shows whether the debug condition is set for exact match or partial match.

Related Commands

Command	Description
call filter match-list voice	Create a call filter match list for debugging voice calls.
debug call filter inout	Display the debug trace inside the GCFM.
debug condition match-list	Run a filtered debug on a voice call.
show call filter components	Display the components used for filtering calls.



show call history fax through show debug condition

- show call history fax, on page 283
- show call history media, on page 293
- show call history stats, on page 302
- show call history video, on page 311
- show call history video record, on page 313
- show call history voice, on page 314
- show call history watermark connected table, on page 320
- show call language voice, on page 322
- show call leg, on page 324
- show call media forking, on page 329
- show callmon, on page 330
- show call prompt-mem-usage, on page 332
- show call resource voice stats, on page 335
- show call resource voice threshold, on page 337
- show call rsvp-sync conf, on page 339
- show call rsvp-sync stats, on page 341
- show call spike status, on page 343
- show call threshold, on page 345
- show call treatment, on page 347
- show call-router routes, on page 350
- show call-router status, on page 352
- show ccm-manager, on page 355
- show cdapi, on page 365
- show ces clock-select, on page 367
- show connect, on page 368
- show controllers rs366, on page 370
- show controllers timeslots, on page 372
- show controllers voice, on page 374
- show crm, on page 377
- show csm, on page 379
- show csm call, on page 386

- show cube debug category codes, on page 388
- show cube status, on page 389
- show debug condition, on page 392

show call history fax

To display the call history table for fax transmissions, use the **show call history fax** command in user EXEC or privileged EXEC mode.

show call history fax [**brief** [**id** *identifier*] | **compact** [**duration** {**less** | **more**} *time*] | **id** *identifier* | **last** *number*]

Syntax Description

brief	(Optional) Displays a truncated version of the call history table.
id *identifier*	(Optional) Displays only the call with the specified identifier. Range is a hex value from 1 to FFFF.
compact	(Optional) Displays a compact version.
duration *time*	(Optional) Displays history information for calls that are longer or shorter than a specified *time* value. The arguments and keywords are as follows: • less--Displays calls shorter than the value in the *time* argument. • more--Displays calls longer than the value in the *time* argument. • *time* --Elapsed time, in seconds. Range is from 1 to 2147483647.
last *number*	(Optional) Displays the last calls connected, where the number of calls that appear is defined by the *number*argument. Range is from 1 to100 .

Command Modes

User EXEC (>)
Privileged EXEC (#)

Command History

Release	Modification
11.3(1)T	This command was introduced on the Cisco 3600 series.
12.0(3)XG	This command was implemented for Voice over Frame Relay (VoFR) on the Cisco 2600 series and Cisco 3600 series.
12.0(4)XJ	This command was modified for store-and-forward fax.
12.0(4)T	This command was modified. The **brief** keyword was added, and the command was implemented on the Cisco 7200 series.
12.0(7)XK	This command was modified. The **brief** keyword was implemented on the Cisco MC3810.
12.1(2)T	This command was integrated into Cisco IOS Release 12.1(2)T.
12.1(5)XM	This command was implemented on the Cisco AS5800.
12.1(5)XM2	This command was implemented on the Cisco AS5350 and Cisco AS5400.

Release	Modification
12.2(2)XA	This command was modified. The output of this command was modified to indicate whether the call in question has been established using Annex E.
12.2(4)T	This command was integrated into Cisco IOS Release 12.2(4)T.
12.2(2)XB1	This command was implemented on the Cisco AS5850.
12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T. Support for the Cisco AS5350, Cisco AS5400, Cisco AS5800, and Cisco AS5850 was not included in this release.
12.2(11)T	This command was implemented on the Cisco AS5350, Cisco AS5400, Cisco AS5800, and Cisco AS5850.
12.3(1)	This command was modified. The following fields were added: FaxRelayMaxJitterBufDepth, FaxRelayJitterBufOverFlow, FaxRelayHSmodulation, and FaxRelayNumberOfPages.
12.3(14)T	This command was modified. T.38 fax relay call statistics were made available to Call Detail Records (CDRs) through vendor-specific attributes (VSAs) and added to the call log.
12.4(15)T	This command was modified. The Port and BearerChannel display fields were added to the TELE call leg record of the command output.
12.4(16)	This command was modified. The Port and BearerChannel display fields were added to the TELE call leg record of the command output.
12.4(22)T	This command was modified. Command output was updated to show IPv6 information.

Usage Guidelines

This command displays a call-history table that contains a list of fax calls connected through the router in descending time order. The maximum number of calls contained in the table can be set to a number from 0 to 500 using the **dial-control-mib** command in global configuration mode. The default maximum number of table entries is 50. Each call record is aged out of the table after a configurable number of minutes has elapsed, also specified by the **dial-control-mib** command. The default timer value is 15 minutes.

You can display subsets of the call history table by using specific keywords. To display the last calls connected through this router, use the keyword **last**, and define the number of calls to be displayed with the number argument.

To display a truncated version of the call history table, use the **brief** keyword.

This command applies to both on-ramp and off-ramp store-and-forward fax functions.

Examples

The following is sample output from the **show call history fax** command:

```
Router# show call history fax
Telephony call-legs: 1
SIP call-legs: 0
H323 call-legs: 0
MGCP call-legs: 0
Total call-legs: 1
GENERIC:
SetupTime=590180 ms
Index=2
PeerAddress=4085452930
```

```
PeerSubAddress=
PeerId=81
PeerIfIndex=221
LogicalIfIndex=145
DisconnectCause=10
DisconnectText=normal call clearing (16)
ConnectTime=59389
DisconnectTime=68204
CallDuration=00:01:28
CallOrigin=2
ReleaseSource=1
ChargedUnits=0
InfoType=fax
TransmitPackets=295
TransmitBytes=5292
ReceivePackets=2967
ReceiveBytes=82110
TELE:
ConnectionId=[0xD9ACDFF1 0x9F5D11D7 0x8002CF18 0xB9C3632]
IncomingConnectionId=[0xD9ACDFF1 0x9F5D11D7 0x8002CF18 0xB9C3632]
CallID=2
Port=3/0/0 (2)
BearerChannel=3/0/0.1
TxDuration=28960 ms
VoiceTxDuration=0 ms
FaxTxDuration=28960 ms
FaxRate=voice bps
FaxRelayMaxJitterBufDepth  = 0 ms
FaxRelayJitterBufOverFlow = 0
FaxRelayHSmodulation = 0
FaxRelayNumberOfPages = 0
NoiseLevel=-120
ACOMLevel=127
SessionTarget=
ImgPages=0
CallerName=
CallerIDBlocked=False
OriginalCallingNumber=4085550130
OriginalCallingOctet=0x0
OriginalCalledNumber=52930
OriginalCalledOctet=0xE9
OriginalRedirectCalledNumber=
OriginalRedirectCalledOctet=0xFF
TranslatedCallingNumber=4085550130
TranslatedCallingOctet=0x0
TranslatedCalledNumber=52930
TranslatedCalledOctet=0xE9
TranslatedRedirectCalledNumber=
TranslatedRedirectCalledOctet=0xFF
GwReceivedCalledNumber=52930
GwReceivedCalledOctet3=0xE9
GwReceivedCallingNumber=4085550130
GwReceivedCallingOctet3=0x0
GwReceivedCallingOctet3a=0x80
```

The table below provides an alphabetical listing of the fields displayed in the output of the **show call history fax** command and a description of each field.

Table 34: show call history fax Field Descriptions

Field	Description
ACOM Level	Current ACOM level for this call. ACOM is the combined loss achieved by the echo canceler, which is the sum of the Echo Return Loss, Echo Return Loss Enhancement, and nonlinear processing loss for the call.
BearerChannel	Identification of the bearer channel carrying the call.
Buffer Drain Events	Total number of jitter buffer drain events.
Buffer Fill Events	Total number of jitter buffer fill events.
CallDuration	Length of the call, in hours, minutes, and seconds, hh:mm:ss.
CallerName	Voice port station name string.
CallOrigin	Call origin: answer or originate.
CallState	Current state of the call.
ChargedUnits	Total number of charging units that apply to this peer since system startup. The unit of measure for this field is hundredths of second.
CodecBytes	Payload size, in bytes, for the codec used.
CoderTypeRate	Negotiated coder rate. This value specifies the send rate of voice or fax compression to its associated call leg for this call.
ConnectionId	Global call identifier for this gateway call.
ConnectTime	Time, in milliseconds (ms), at which the call was connected.
Consecutive-packets-lost Events	Total number of consecutive (two or more) packet-loss events.
Corrected packet-loss Events	Total number of packet-loss events that were corrected using the RFC 2198 method.
Dial-Peer	Tag of the dial peer sending this call.
DisconnectCause	Cause code for the reason this call was disconnected.
DisconnectText	Descriptive text explaining the reason for the disconnect.
DisconnectTime	Time, in ms, when this call was disconnected.
EchoCancellerMaxReflector=64	The location of the largest reflector, in ms. The reflector size does not exceed the configured echo path capacity. For example, if 32 ms is configured, the reflector does not report beyond 32 ms.
ERLLevel	Current Echo Return Loss (ERL) level for this call.
FaxTxDuration	Duration of fax transmission from this peer to the voice gateway for this call. You can derive the Fax Utilization Rate by dividing the FaxTxDuration value by the TxDuration value.

Field	Description
FaxRelayJitterBufOverFlow	Count of number of network jitter buffer overflows (number of packets). These packets are equivalent to lost packets.
FaxRelayMaxJitterBufDepth	Maximum depth of jitter buffer (in ms).
FaxRelayHSmodulation	Most recent high-speed modulation used.
FaxRelayNumberOfPages	Number of pages transmitted.
GapFillWithInterpolation	Duration of a voice signal played out with a signal synthesized from parameters, or samples of data preceding and following in time because voice data was lost or not received in time from the voice gateway for this call.
GapFillWithRedundancy	Duration of a voice signal played out with a signal synthesized from available redundancy parameters because voice data was lost or not received in time from the voice gateway for this call.
GapFillWithPrediction	Duration of the voice signal played out with signal synthesized from parameters, or samples of data preceding in time, because voice data was lost or not received in time from the voice gateway for this call. Examples of such pullout are frame-eraser and frame-concealment strategies in G.729 and G.723.1 compression algorithms.
GapFillWithSilence	Duration of a voice signal replaced with silence because voice data was lost or not received in time for this call.
GENERIC	Generic or common parameters, that is, parameters that are common for VoIP and telephony call legs.
GwReceivedCalledNumber, GwReceivedCalledOctet3, GwReceivedCallingNumber, GwReceivedCallingOctet3, GwReceivedCallingOctet3a	Call information received at the gateway.
H323 call-legs	Total H.323 call legs for which call records are available.
HiWaterPlayoutDelay	High-water-mark Voice Playout FIFO Delay during this call.
ImgPages	The fax pages that have been processed.
Incoming ConnectionId	The incoming_GUID. It can be different with ConnectionId (GUID) when there is a long_pound or blast_call feature involved. In those cases, incoming_GUID is unique for all the subcalls that have been generated, and GUID is different for each subcall.
Index	Dial peer identification number.
InfoActivity	Active information transfer activity state for this call.
InfoType	Information type for this call; for example, voice or fax.

Field	Description
InSignalLevel	Active input signal level from the telephony interface used by this call.
Last Buffer Drain/Fill Event	Elapsed time since the last jitter buffer drain or fill event, in seconds.
Local UUID	Unique identifier generated from the originating user agent.
LogicalIfIndex	Index number of the logical interface for this call.
LoWaterPlayoutDelay	Low-water-mark Voice Playout FIFO Delay during this call.
LowerIFName	Physical lower interface information. Appears only if the medium is ATM, Frame Relay (FR), or High-Level Data Link Control (HDLC).
Media	Medium over which the call is carried. If the call is carried over the (telephone) access side, the entry is TELE. If the call is carried over the voice network side, the entry is either ATM, FR, or HDLC.
Modem passthrough signaling method in use	Indicates that this is a modem pass-through call and that named signaling events (NSEs)--a Cisco-proprietary version of named telephone events in RFC 2833--are used for signaling codec upspeed. The upspeed method is the method used to dynamically change the codec type and speed to meet network conditions. This means that you might move to a faster codec when you have both voice and data calls and then slow down when there is only voice traffic.
NoiseLevel	Active noise level for this call.
OnTimeRvPlayout	Duration of voice playout from data received on time for this call. Derive the Total Voice Playout Duration for Active Voice by adding the OnTimeRvPlayout value to the GapFill values.
OriginalCallingNumber, OriginalCalling Octet, OriginalCalledNumber, OriginalCalledOctet, OriginalRedirectCalledNumber, OriginalRedirectCalledOctet	Original call information regarding calling, called, and redirect numbers, as well as octet-3s. Octet-3s are information elements (IEs) of Q.931 that include type of number, numbering plan indicator, presentation indicator, and redirect reason information.
OutSignalLevel	Active output signal level to the telephony interface used by this call.
PeerAddress	Destination pattern or number associated with this peer.
PeerId	ID value of the peer table entry to which this call was made.
PeerIfIndex	Voice port index number for this peer. For ISDN media, this would be the index number of the B channel used for this call.
PeerSubAddress	Subaddress when this call is connected.
Percent Packet Loss	Total percent packet loss.
Port	Identification of the voice port carrying the call.

Field	Description
ReceiveBytes	Number of bytes received by the peer during this call.
ReceiveDelay	Average Playout FIFO Delay plus the Decoder Delay during this voice call.
ReceivePackets	Number of packets received by this peer during this call.
ReleaseSource	Number value of the release source.
RemoteIPAddress	Remote system IP address for the VoIP call.
RemoteUDPPort	Remote system User Datagram Protocol (UDP) listener port to which voice packets are sent.
Remote UUID	Unique identifier generated from the terminating user agent.
RoundTripDelay	Voice packet round-trip delay between the local and remote systems on the IP backbone for this call.
SelectedQoS	Selected Resource Reservation Protocol (RSVP) quality of service (QoS) for this call.
SessionProtocol	Session protocol used for an Internet call between the local and remote routers through the IP backbone.
SessionTarget	Session target of the peer used for this call.
SetupTime	Value of the system UpTime, in ms, when the call associated with this entry was started.
SignalingType	Signaling type for this call; for example, channel-associated signaling (CAS) or common-channel signaling (CCS).
SIP call-legs	Total SIP call legs for which call records are available.
Telephony call-legs	Total telephony call legs for which call records are available.
Time between Buffer Drain/Fills	Minimum and maximum durations between jitter buffer drain or fill events, in seconds.
TranslatedCallingNumber, TranslatedCallingOctet, TranslatedCalledNumber, TranslatedCalledOctet, TranslatedRedirectCalled Number, TranslatedRedirectCalledOctet	Translated call information.
TransmitBytes	Number of bytes sent by this peer during this call.
TransmitPackets	Number of packets sent by this peer during this call.
TxDuration	The length of the call. Appears only if the medium is TELE.

Field	Description
VAD	Whether voice activation detection (VAD) was enabled for this call.
VoiceTxDuration	Duration of voice transmission from this peer to the voice gateway for this call. Derive the Voice Utilization Rate by dividing the VoiceTxDuration value by the TxDuration value.

The following is sample output from the **show call history fax brief**command:

```
Router# show call history fax brief
<ID>: <start>hs.<index> +<connect> +<disc> pid:<peer_id> <direction> <addr>
 tx:<packets>/<bytes> rx:<packets>/<bytes> <disc-cause>(<text>)
 IP <ip>:<udp> rtt:<time>ms pl:<play>/<gap>ms lost:<lost>/<early>/<late>
  delay:<last>/<min>/<max>ms <codec>
 Telephony <int>: tx:<tot>/<voice>/<fax>ms <codec> noise:<lvl>dBm acom:<lvl>dBm
2    : 5996450hs.25 +-1 +3802 pid:100 Answer 408
 tx:0/0 rx:0/0 1F  (T30 T1 EOM timeout)
 Telephony : tx:38020/38020/0ms g729r8 noise:0dBm acom:0dBm
2    : 5996752hs.26 +-1 +3500 pid:110 Originate uut1@linux2.allegro.com
 tx:0/0 rx:0/0 3F  (The e-mail was not sent correctly. Remote SMTP server said: 354 )
 IP 14.0.0.1 AcceptedMime:0 DiscardedMime:0
3    : 6447851hs.27 +1111 +3616 pid:310 Originate 576341.
 tx:11/14419 rx:0/0 10  (Normal connection)
 Telephony : tx:36160/11110/25050ms g729r8 noise:115dBm acom:-14dBm
3    : 6447780hs.28 +1182 +4516 pid:0 Answer
 tx:0/0 rx:0/0 10  (normal call clearing.)
 IP 0.0.0.0 AcceptedMime:0 DiscardedMime:0
4    : 6464816hs.29 +1050 +3555 pid:310 Originate 576341.
 tx:11/14413 rx:0/0 10  (Normal connection)
 Telephony : tx:35550/10500/25050ms g729r8 noise:115dBm acom:-14dBm
4    : 6464748hs.30 +1118 +4517 pid:0 Answer
 tx:0/0 rx:0/0 10  (normal call clearing.)
 IP 0.0.0.0 AcceptedMime:0 DiscardedMime:0
5    : 6507900hs.31 +1158 +2392 pid:100 Answer 4085763413
 tx:0/0 rx:3/3224 10  (Normal connection)
 Telephony : tx:23920/11580/12340ms g729r8 noise:0dBm acom:0dBm
5    : 6508152hs.32 +1727 +2140 pid:110 Originate uut1@linux2.allegro.com
 tx:0/2754 rx:0/0 3F  (service or option not available, unspecified)
 IP 14.0.0.4 AcceptedMime:0 DiscardedMime:0
6    : 6517176hs.33 +1079 +3571 pid:310 Originate 576341.
 tx:11/14447 rx:0/0 10  (Normal connection)
 Telephony : tx:35710/10790/24920ms g729r8 noise:115dBm acom:-14dBm
6    : 6517106hs.34 +1149 +4517 pid:0 Answer
 tx:0/0 rx:0/0 10  (normal call clearing.)
 IP 0.0.0.0 AcceptedMime:0 DiscardedMime:0
7    : 6567382hs.35 +1054 +3550 pid:310 Originate 576341.
 tx:11/14411 rx:0/0 10  (Normal connection)
 Telephony : tx:35500/10540/24960ms g729r8 noise:115dBm acom:-14dBm
7    : 6567308hs.36 +1128 +4517 pid:0 Answer
tx:0/0 rx:0/0 10  (normal call clearing.)
 IP 0.0.0.0 AcceptedMime:0 DiscardedMime:0
```

The following example shows output for the **show call history fax** command with the T.38 Fax Relay statistics:

```
Router# show call history fax
Telephony call-legs: 1
SIP call-legs: 0
H323 call-legs: 0
MGCP call-legs: 0
```

```
Total call-legs: 1
GENERIC:
SetupTime=9872460 ms
Index=8
PeerAddress=41023
PeerSubAddress=
PeerId=1
PeerIfIndex=242
LogicalIfIndex=180
DisconnectCause=10
DisconnectText=normal call clearing (16)
ConnectTime=9875610 ms
DisconnectTime=9936000 ms
CallDuration=00:01:00 sec
CallOrigin=2
ReleaseSource=1
ChargedUnits=0
InfoType=fax
TransmitPackets=268
TransmitBytes=4477
ReceivePackets=1650
ReceiveBytes=66882
TELE:
ConnectionId=[0xD6635DD5 0x9FA411D8 0x8005000A 0xF4107CA0]
IncomingConnectionId=[0xD6635DD5 0x9FA411D8 0x8005000A 0xF4107CA0]
CallID=7
Port=3/0/0:0 (7)
BearerChannel=3/0/0.8
TxDuration=6170 ms
VoiceTxDuration=0 ms
FaxTxDuration=0 ms
FaxRate=disable bps
FaxRelayMaxJitterBufDepth=560 ms
FaxRelayJitterBufOverFlow=0
FaxRelayMostRecentHSmodulation=V.17/short/14400
FaxRelayNumberOfPages=1
FaxRelayInitHSmodulation=V.17/long/14400
FaxRelayDirection=Transmit
FaxRelayPktLossConceal=0
FaxRelayEcmStatus=ENABLED
FaxRelayEncapProtocol=T.38 (UDPTL)
FaxRelayNsfCountryCode=Japan
FaxRelayNsfManufCode=0031B8EE80C48511DD0D0000DDDD0000DDDD00000000000000000022ED00B0A400
FaxRelayFaxSuccess=Success
NoiseLevel=0
ACOMLevel=0
SessionTarget=
ImgPages=0
CallerName=Analog 41023
CallerIDBlocked=False
OriginalCallingNumber=
OriginalCallingOctet=0x80
OriginalCalledNumber=41021
OriginalCalledOctet=0xA1
OriginalRedirectCalledNumber=
OriginalRedirectCalledOctet=0xFF
TranslatedCallingNumber=41023
TranslatedCallingOctet=0x80
TranslatedCalledNumber=41021
TranslatedCalledOctet=0xA1
TranslatedRedirectCalledNumber=
TranslatedRedirectCalledOctet=0xFF
GwReceivedCalledNumber=41021
GwReceivedCalledOctet3=0xA1
```

The table below describes the fields not shown in the table above.

Table 35: show call history fax Field Descriptions

Field	Description
FaxRelayDirection	Direction of fax relay.
FaxRelayEcmStatus	Fax relay error correction mode status.
FaxRelayEncapProtocol	Fax relay encapsulation protocol.
FaxRelayFaxSuccess	Fax relay success.
FaxRelayInitHSmodulation	Fax relay initial high speed modulation.
FaxRelayMostRecentHSmodulation	Fax relay most recent high speed modulation.
FaxRelayNsfCountryCode	Fax relay Nonstandard Facilities (NSF) country code.
FaxRelayNsfManufCode	Fax relay NSF manufacturers code.
FaxRelayPktLossConceal	Fax relay packet loss conceal.

Related Commands

Command	Description
dial-control-mib	Specifies attributes for the call history table.
show call active fax	Displays call information for fax transmissions that are in progress.
show call active voice	Displays call information for voice calls that are in progress.
show call history voice	Displays the call history table for voice calls.
show dial-peer voice	Displays configuration information for dial peers.
show num-exp	Displays how the number expansions are configured in VoIP.
show voice port	Displays configuration information about a specific voice port.

show call history media

To display the call history table for media calls, use the **show call history media**command in user EXEC or privileged EXEC mode.

show call history media [[**brief**] [**id** *identifier*] | **compact** [**duration** {**less** | **more**} *seconds*] | **last** *number*]

Syntax Description

brief	(Optional) Displays a truncated version of the call history table.
id *identifier*	(Optional) Displays only the call with the specified *identifier*. The range is from 1 to FFFF.
compact	(Optional) Displays a compact version of the call history table.
duration	(Optional) Displays the call history for the specified time duration.
less	Displays the call history for shorter duration calls.
more	Displays the call history for longer duration calls.
seconds	Time, in seconds. The range is from 1 to 2147483647.
last *number*	(Optional) Displays the last calls connected, where the number of calls that appear is defined by the *number*argument. The range is from 1 to100 .

Command Modes

User EXEC (>)
Privileged EXEC (#)

Command History

Release	Modification
12.4(15)T	This command was introduced.

Usage Guidelines

This command displays a call-history table that contains a list of media calls connected through the router in descending time order. The maximum number of calls contained in the table can be set to a number from 0 to 500 using the **dial-control-mib** command in global configuration mode. The default maximum number of table entries is 50. Each call record is aged out of the table after a configurable number of minutes has elapsed, also specified by the **dial-control-mib** command. The default timer value is 15 minutes.

You can display subsets of the call history table by using specific keywords. To display the last calls connected through this router, use the **last** keyword, and define the number of calls to be displayed with the *number* argument.

To display a truncated version of the call history table, use the **brief** keyword.

When a media call is active, you can display its statistics by using the **show call active media** command.

Examples

The following is sample output from the **show call history media**command:

```
Router# show call history media
Telephony call-legs: 0
```

```
SIP call-legs: 0
H323 call-legs: 0
Call agent controlled call-legs: 0
Media call-legs: 4
Total call-legs: 4
GENERIC:
SetupTime=308530 ms
Index=4
PeerAddress=sip:mrcpv2ASRServer@10.5.18.224:5060
PeerSubAddress=
PeerId=2234
PeerIfIndex=184
LogicalIfIndex=0
DisconnectCause=10
DisconnectText=normal call clearing (16)
ConnectTime=309440 ms
DisconnectTime=320100 ms
CallDuration=00:00:10 sec
CallOrigin=1
ReleaseSource=7
ChargedUnits=0
InfoType=speech
TransmitPackets=237
TransmitBytes=37920
ReceivePackets=0
ReceiveBytes=0
VOIP:
ConnectionId[0x2FB5B737 0xC3511DB 0x8005000B 0x5FDA0EF4]
IncomingConnectionId[0x2FB5B737 0xC3511DB 0x8005000B 0x5FDA0EF4]
CallID=14
RemoteIPAddress=10.5.18.224
RemoteUDPPort=10002
RemoteSignallingIPAddress=10.5.18.224
RemoteSignallingPort=5060
RemoteMediaIPAddress=10.5.18.224
RemoteMediaPort=10002
SRTP = off
TextRelay = off
Fallback Icpif=0
Fallback Loss=0
Fallback Delay=0
RoundTripDelay=0 ms
SelectedQoS=best-effort
tx_DtmfRelay=rtp-nte
FastConnect=FALSE
AnnexE=FALSE
Separate H245 Connection=FALSE
H245 Tunneling=FALSE
SessionProtocol=sipv2
ProtocolCallId=2FBDA670-C3511DB-8015C48C-6A894889@10.5.14.2
SessionTarget=10.5.18.224
OnTimeRvPlayout=3000
GapFillWithSilence=0 ms
GapFillWithPrediction=0 ms
GapFillWithInterpolation=2740 ms
GapFillWithRedundancy=0 ms
HiWaterPlayoutDelay=100 ms
LoWaterPlayoutDelay=40 ms
Source tg label=test5
ReceiveDelay=90 ms
LostPackets=0
EarlyPackets=0
LatePackets=0
VAD = disabled
```

```
CoderTypeRate=g711ulaw
CodecBytes=160
cvVoIPCallHistoryIcpif=16
MediaSetting=flow-around
CallerName=
CallerIDBlocked=False
OriginalCallingNumber=
OriginalCallingOctet=0x0
OriginalCalledNumber=
OriginalCalledOctet=0x0
OriginalRedirectCalledNumber=
OriginalRedirectCalledOctet=0x0
TranslatedCallingNumber=555-0100
TranslatedCallingOctet=0x21
TranslatedCalledNumber=
TranslatedCalledOctet=0xC1
TranslatedRedirectCalledNumber=
TranslatedRedirectCalledOctet=0xFF
GwOutpulsedCallingNumber=555-0101
GwOutpulsedCallingOctet3=0x21
GwOutpulsedCallingOctet3a=0x81
MediaInactiveDetected=no
MediaInactiveTimestamp=
MediaControlReceived=
LongDurationCallDetected=no
LongDurationCallTimerStamp=
LongDurationCallDuration=
Username=
GENERIC:
SetupTime=308520 ms
Index=5
PeerAddress=sip:mrcpv2TTSServer@10.5.18.224:5060
PeerSubAddress=
PeerId=2235
PeerIfIndex=185
LogicalIfIndex=0
DisconnectCause=10
DisconnectText=normal call clearing (16)
ConnectTime=309370 ms
DisconnectTime=320100 ms
CallDuration=00:00:10 sec
CallOrigin=1
ReleaseSource=7
ChargedUnits=0
InfoType=speech
TransmitPackets=0
TransmitBytes=0
ReceivePackets=551
ReceiveBytes=88160
VOIP:
ConnectionId[0x2FB5B737 0xC3511DB 0x8005000B 0x5FDA0EF4]
IncomingConnectionId[0x2FB5B737 0xC3511DB 0x8005000B 0x5FDA0EF4]
CallID=13
RemoteIPAddress=10.5.18.224
RemoteUDPPort=10000
RemoteSignallingIPAddress=10.5.18.224
RemoteSignallingPort=5060
RemoteMediaIPAddress=10.5.18.224
RemoteMediaPort=10000
SRTP = off
TextRelay = off
Fallback Icpif=0
Fallback Loss=0
Fallback Delay=0
```

```
RoundTripDelay=0 ms
SelectedQoS=best-effort
tx_DtmfRelay=rtp-nte
FastConnect=FALSE
AnnexE=FALSE
Separate H245 Connection=FALSE
H245 Tunneling=FALSE
SessionProtocol=sipv2
ProtocolCallId=2FBC6E20-C3511DB-8013C48C-6A894889@10.5.14.2
SessionTarget=10.5.18.224
OnTimeRvPlayout=7000
GapFillWithSilence=0 ms
GapFillWithPrediction=0 ms
GapFillWithInterpolation=2740 ms
GapFillWithRedundancy=0 ms
HiWaterPlayoutDelay=100 ms
LoWaterPlayoutDelay=40 ms
Source tg label=test5
ReceiveDelay=95 ms
LostPackets=0
EarlyPackets=0
LatePackets=0
VAD = disabled
CoderTypeRate=g711ulaw
CodecBytes=160
cvVoIPCallHistoryIcpif=16
MediaSetting=flow-around
CallerName=
CallerIDBlocked=False
OriginalCallingNumber=
OriginalCallingOctet=0x0
OriginalCalledNumber=
OriginalCalledOctet=0x0
OriginalRedirectCalledNumber=
OriginalRedirectCalledOctet=0x0
TranslatedCallingNumber=555-0102
TranslatedCallingOctet=0x21
TranslatedCalledNumber=
TranslatedCalledOctet=0xC1
TranslatedRedirectCalledNumber=
TranslatedRedirectCalledOctet=0xFF
GwOutpulsedCallingNumber=555-0103
GwOutpulsedCallingOctet3=0x21
GwOutpulsedCallingOctet3a=0x81
MediaInactiveDetected=no
MediaInactiveTimestamp=
MediaControlReceived=
LongDurationCallDetected=no
LongDurationCallTimerStamp=
LongDurationCallDuration=
Username=
GENERIC:
SetupTime=408050 ms
Index=7
PeerAddress=sip:mrcpv2ASRServer@10.5.18.224:5060
PeerSubAddress=
PeerId=2234
PeerIfIndex=184
LogicalIfIndex=0
DisconnectCause=10
DisconnectText=normal call clearing (16)
ConnectTime=408160 ms
DisconnectTime=426260 ms
CallDuration=00:00:18 sec
```

```
CallOrigin=1
ReleaseSource=7
ChargedUnits=0
InfoType=speech
TransmitPackets=598
TransmitBytes=95680
ReceivePackets=0
ReceiveBytes=0
VOIP:
ConnectionId[0x6B02FC0C 0xC3511DB 0x8006000B 0x5FDA0EF4]
IncomingConnectionId[0x6B02FC0C 0xC3511DB 0x8006000B 0x5FDA0EF4]
CallID=19
RemoteIPAddress=10.5.18.224
RemoteUDPPort=10002
RemoteSignallingIPAddress=10.5.18.224
RemoteSignallingPort=5060
RemoteMediaIPAddress=10.5.18.224
RemoteMediaPort=10002
SRTP = off
TextRelay = off
Fallback Icpif=0
Fallback Loss=0
Fallback Delay=0
RoundTripDelay=0 ms
SelectedQoS=best-effort
tx_DtmfRelay=rtp-nte
FastConnect=FALSE
AnnexE=FALSE
Separate H245 Connection=FALSE
H245 Tunneling=FALSE
SessionProtocol=sipv2
ProtocolCallId=6B0E94CD-C3511DB-801DC48C-6A894889@10.5.14.2
SessionTarget=10.5.18.224
OnTimeRvPlayout=11000
GapFillWithSilence=0 ms
GapFillWithPrediction=0 ms
GapFillWithInterpolation=9560 ms
GapFillWithRedundancy=0 ms
HiWaterPlayoutDelay=100 ms
LoWaterPlayoutDelay=55 ms
Source tg label=test5
ReceiveDelay=100 ms
LostPackets=0
EarlyPackets=0
LatePackets=0
VAD = disabled
CoderTypeRate=g711ulaw
CodecBytes=160
cvVoIPCallHistoryIcpif=16
MediaSetting=flow-around
CallerName=
CallerIDBlocked=False
OriginalCallingNumber=
OriginalCallingOctet=0x0
OriginalCalledNumber=
OriginalCalledOctet=0x0
OriginalRedirectCalledNumber=
OriginalRedirectCalledOctet=0x0
TranslatedCallingNumber=555-0100
TranslatedCallingOctet=0x21
TranslatedCalledNumber=
TranslatedCalledOctet=0xC1
TranslatedRedirectCalledNumber=
TranslatedRedirectCalledOctet=0xFF
```

```
GwOutpulsedCallingNumber=555-0101
GwOutpulsedCallingOctet3=0x21
GwOutpulsedCallingOctet3a=0x81
MediaInactiveDetected=no
MediaInactiveTimestamp=
MediaControlReceived=
LongDurationCallDetected=no
LongDurationCallTimerStamp=
LongDurationCallDuration=
Username=
GENERIC:
SetupTime=408040 ms
Index=8
PeerAddress=sip:mrcpv2TTSServer@10.5.18.224:5060
PeerSubAddress=
PeerId=2235
PeerIfIndex=185
LogicalIfIndex=0
DisconnectCause=10
DisconnectText=normal call clearing (16)
ConnectTime=408130 ms
DisconnectTime=426260 ms
CallDuration=00:00:18 sec
CallOrigin=1
ReleaseSource=7
ChargedUnits=0
InfoType=speech
TransmitPackets=0
TransmitBytes=0
ReceivePackets=911
ReceiveBytes=145760
VOIP:
ConnectionId[0x6B02FC0C 0xC3511DB 0x8006000B 0x5FDA0EF4]
IncomingConnectionId[0x6B02FC0C 0xC3511DB 0x8006000B 0x5FDA0EF4]
CallID=18
RemoteIPAddress=10.5.18.224
RemoteUDPPort=10000
RemoteSignallingIPAddress=10.5.18.224
RemoteSignallingPort=5060
RemoteMediaIPAddress=10.5.18.224
RemoteMediaPort=10000
SRTP = off
TextRelay = off
Fallback Icpif=0
Fallback Loss=0
Fallback Delay=0
RoundTripDelay=0 ms
SelectedQoS=best-effort
tx_DtmfRelay=rtp-nte
FastConnect=FALSE
AnnexE=FALSE
Separate H245 Connection=FALSE
H245 Tunneling=FALSE
SessionProtocol=sipv2
ProtocolCallId=6B0CC055-C3511DB-801BC48C-6A894889@10.5.14.2
SessionTarget=10.5.18.224
OnTimeRvPlayout=9000
GapFillWithSilence=0 ms
GapFillWithPrediction=0 ms
GapFillWithInterpolation=9560 ms
GapFillWithRedundancy=0 ms
HiWaterPlayoutDelay=100 ms
LoWaterPlayoutDelay=55 ms
Source tg label=test5
```

```
ReceiveDelay=100 ms
LostPackets=0
EarlyPackets=0
LatePackets=0
VAD = disabled
CoderTypeRate=g711ulaw
CodecBytes=160
cvVoIPCallHistoryIcpif=16
MediaSetting=flow-around
CallerName=
CallerIDBlocked=False
OriginalCallingNumber=
OriginalCallingOctet=0x0
OriginalCalledNumber=
OriginalCalledOctet=0x0
OriginalRedirectCalledNumber=
OriginalRedirectCalledOctet=0x0
TranslatedCallingNumber=555-0100
TranslatedCallingOctet=0x21
TranslatedCalledNumber=
TranslatedCalledOctet=0xC1
TranslatedRedirectCalledNumber=
TranslatedRedirectCalledOctet=0xFF
GwOutpulsedCallingNumber=555-0101
GwOutpulsedCallingOctet3=0x21
GwOutpulsedCallingOctet3a=0x81
MediaInactiveDetected=no
MediaInactiveTimestamp=
MediaControlReceived=
LongDurationCallDetected=no
LongDurationCallTimerStamp=
LongDurationCallDuration=
Username=
```

The table below describes the significant fields shown in the display, in alphabetical order.

Table 36: show call history media Field Descriptions

Field	Description
CallDuration	Length of the call, in hours, minutes, and seconds, hh:mm:ss.
CallOrigin	Call origin: not answer or originate.
ChargedUnits	Total number of charging units that apply to this peer since system startup. The unit of measure for this field is hundredths of second.
CodecBytes	Payload size, in bytes, for the codec used.
CoderTypeRate	Negotiated coder rate. This value specifies the send rate of voice or fax compression to its associated call leg for this call.
ConnectionId	Global call identifier for this gateway call.
ConnectTime	Time, in ms, during which the call was connected.
GapFillWithInterpolation	Duration, in ms, of a voice signal played out with a signal synthesized from parameters, or samples of data preceding and following in time because voice data was lost or not received in time from the voice gateway for this call.

Field	Description
GapFillWithRedundancy	Duration, in ms, of a voice signal played out with a signal synthesized from available redundancy parameters because voice data was lost or not received in time from the voice gateway for this call.
GapFillWithPrediction	Duration, in ms, of the voice signal played out with a signal synthesized from parameters, or samples of data preceding in time, because voice data was lost or not received in time from the voice gateway for this call. Examples of such pullout are frame-eraser and frame-concealment strategies in G.729 and G.723.1 compression algorithms.
GapFillWithSilence	Duration, in ms, of a voice signal replaced with silence because voice data was lost or not received in time for this call.
GENERIC	Generic or common parameters; that is, parameters that are common for VoIP and telephony call legs.
H323 call-legs	Total H.323 call legs for which call records are available.
HiWaterPlayoutDelay	High-water-mark voice playout first in first out (FIFO) Delay during this call, in ms.
Index	Dial peer identification number.
InfoType	Information type for this call; for example, voice, speech, or fax.
LogicalIfIndex	Index number of the logical interface for this call.
LoWaterPlayoutDelay	Low-water-mark voice playout FIFO delay during this call, in ms.
OnTimeRvPlayout	Duration of voice playout from data received on time for this call. Derive the Total Voice Playout Duration for Active Voice by adding the OnTimeRvPlayout value to the GapFill values.
PeerAddress	Destination pattern or number associated with this peer.
PeerId	ID value of the peer table entry to which this call was made.
PeerIfIndex	Voice port index number for this peer. For ISDN media, this would be the index number of the B channel used for this call.
PeerSubAddress	Subaddress when this call is connected.
ReceiveBytes	Number of bytes received by the peer during this call.
ReceiveDelay	Average playout FIFO delay plus the decoder delay during this voice call, in ms.
ReceivePackets	Number of packets received by this peer during this call.
ReleaseSource	Number value of the release source.
RemoteIPAddress	Remote system IP address for the VoIP call.

Field	Description
RemoteUDPPort	Remote system User Datagram Protocol (UDP) listener port to which voice packets are sent.
RoundTripDelay	Voice packet round-trip delay, in ms, between the local and remote systems on the IP backbone for this call.
SelectedQoS	Selected Resource Reservation Protocol (RSVP) quality of service (QoS) for this call.
SessionProtocol	Session protocol used for an Internet call between the local and remote routers through the IP backbone.
SessionTarget	Session target of the peer used for this call.
SetupTime	Value of the system UpTime, in ms, when the call associated with this entry was started.
SIP call-legs	Total Session Initiation Protocol (SIP) call legs for which call records are available.
Telephony call-legs	Total telephony call legs for which call records are available.
TransmitBytes	Number of bytes sent by this peer during this call.
TransmitPackets	Number of packets sent by this peer during this call.
VAD	Whether voice activation detection (VAD) was enabled for this call.

Related Commands

Command	Description
dial-control-mib	Sets the maximum number of calls contained in the table.
show call active media	Displays call information for media calls in progress.

show call history stats

To display the statistics of call history, use **show call history stats** command in privileged EXEC mode.

show call history stats {**connected** *table* | **cps** { *details* | *table* } | **short-duration**

Syntax Description

connected	Displays call statistics for connected calls.
table	(Optional) Displays call statistics for connected calls in tabular format.
cps	Displays call statistics in calls handled per second format.
details	Displays call statistics in calls handled per second format including call-leg rate.
table	Displays call statistics in calls handled per second format including call-leg rate in tabular format
short-duration	Displays the call statistics for short-duration calls. By default, any call with total duration less than 5 seconds is considered as a short duration call. You can change the default value using Management Information Base (MIB).

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Release 3.8	This command was introduced.

Usage Guidelines

Use **show call history stats connected** command to display statistics of connected calls in graphical format.

```
Device#show call history stats connected


   10
    9
    8
    7
    6
    5
    4
    3
    2
    1
     0....5....1....1....2....2....3....3....4....4....5....5....6
               0    5    0    5    0    5    0    5    0    5    0
          Connected Calls (last 60 seconds)
          # = Connected calls handled by the module



                                                      369963146641
                                                     8880000440044
                                                     8880077990066
  910                                                   **
  820                                                   #*
```

```
730                                                  *##
640                                                  *##*   **
550                                                  ###*   ##
460                                                  ####  *##*
370                                                 *####  *##*
280                                                 #####* ####
190                                                 ######*####*
100                                                *######*####*
 10                                                ##############
   0....5....1....1....2....2....3....3....4....4....5....5....6
             0    5    0    5    0    5    0    5    0    5    0
        Connected Calls (last 60 minutes)
        * = maximum Connected calls    # = average Connected calls



    9
    0
    0
970
890 *
810 *
730 *
650 *
570 *
490 *
410 *
330 *
250 *
170 #
   0....5....1....1....2....2....3....3....4....4....5....5....6....6....7..
             0    5    0    5    0    5    0    5    0    5    0    5    0
        Connected Calls (last 72 hours)
        * = maximum Connected calls    # = average Connected calls
```

The following section describes how to interpret the graphical data:

- **Connected calls for the last 60 seconds**—The graph displays the number of connected calls in the last 60 seconds. X-axis represents the time in seconds and Y-axis represents the number of connected calls. **#** represents the number of connected calls.

  For example, in the following graph, 15 calls were connected at the 2nd second.

```
                        1
      1122334455667788990998877665544332211
      5050505050505061505050505050505050505
  100                 ###
   90               #######
   80             ###########
   70           ###############
   60         ###################
   50       #######################
   40     ###########################
   30   ###############################
   20  #################################
   10 ###################################
     0....5....1....1....2....2....3....3....4....4....5....5....6
               0    5    0    5    0    5    0    5    0    5    0
```

- **Connected calls for the last 60 minutes**—The graph displays the number of connected calls in the last 60 minutes. X-axis represents the time in minutes and Y-axis represents the number of connected calls. The values on the Y-axis vary based on the number of connected calls. ***** represents the maximum number of connected calls. **#** represents the average number of connected calls. The maximum number of connected

calls over a minute is calculated by taking the average of 3 maximum values of connected calls over the 60 seconds in that minute.

For example, in the following graph, on the 48th minute, a maximum of 383 calls were connected and average calls were 10.

```
                                                  369863146641
                                                 8880900440044
                                                 3330922440011
910                                                 **
820                                                 #*
730                                                 ##
640                                                *###*   **
550                                                ###*   ##
460                                                ####  *###*
370                                               *####  *###*
280                                               #####* ####
190                                               ###### ####
100                                              *######*#####*
 10                                              ##############
   0....5....1....1....2....2....3....3....4....4....5....5....6
            0    5    0    5    0    5    0    5    0    5    0
        Connected Cube Calls (last 60 minutes)
        * = maximum Connected calls    # = average Connected calls
```

- **Connected calls for the last 72 hours**—The graph displays the number of connected calls in the last 72 hours. X-axis represents the time in hours and Y-axis represents the number of connected calls. The values on the Y-axis vary based on the number of connected calls. ***** represents the maximum number of connected calls. **#** represents the average number of connected calls. The maximum connected calls over each hour are the same as the maximum connected calls over the minutes in that hour.

  For example, in the following graph, during the first hour, a maximum of 900 calls were connected and average calls were 170.

```
    9
    0
    0
970
890 *
810 *
730 *
650 *
570 *
490 *
410 *
330 *
250 *
170 #
   0....5....1....1....2....2....3....3....4....4....5....5....6....6....7..
            0    5    0    5    0    5    0    5    0    5    0    5    0
        Connected Cube Calls (last 72 hours)
        * = maximum Connected calls    # = average Connected calls
```

Use **table** keyword to display the connected call statistics in tabular format. The output includes the following tables:

- Connected calls for the last 60 seconds
- Connected calls for the last 60 minutes

- Connected calls for the last 72 hours

```
Device#show call history stats connected table

   11:01:44 AM Thursday Aug 29 2019 IST


Connected Calls  (last 60 seconds)
Period     Average       Max
---------------------------
 1-5           0          0
 6-10          0          0
11-15          0          0
16-20          0          0
21-25          0          0
26-30          0          0
31-35          0          0
36-40          0          0
41-45          0          0
46-50          0          0
51-55          0          0
56-60          0          0


Connected Calls  (last 60 minutes)
Period     Average       Max
---------------------------
 1-5           0          0
 6-10          0          0
11-15          0          0
16-20          0          0
21-25          0          0
26-30          0          0
31-35          0          0
36-40          0          0
41-45          0          0
46-50        324        900
51-55        343        900
56-60        292        600


Connected Calls  (last 72 hours)
Period     Average       Max
---------------------------
 1-5          35        900
 6-10          0          0
11-15          0          0
16-20          0          0
21-25          0          0
26-30          0          0
31-35          0          0
36-40          0          0
41-45          0          0
46-50          0          0
51-55          0          0
56-60          0          0
61-65          0          0
66-70          0          0
71-72          0          0
```

Example

```
Device#show call history stats cps

   10:26:05 AM Wednesday Sep 25 2019 UTC




  10
   9
   8
   7
   6
   5
   4
   3
   2
   1
    0....5....1....1....2....2....3....3....4....4....5....5....6
              0    5    0    5    0    5    0    5    0    5    0
         Call switching rate / CPS (last 60 seconds)
         # = calls handled by the module per second




                               11
  10
   9
   8
   7
   6
   5
   4
   3
   2
   1                           **
    0....5....1....1....2....2....3....3....4....4....5....5....6
              0    5    0    5    0    5    0    5    0    5    0
         Call switching rate / CPS  (last 60 minutes)
         * = maximum calls/s    # = average calls/s




     1
  10
   9
   8
   7
   6
   5
   4
   3
   2
   1 *
    0....5....1....1....2....2....3....3....4....4....5....5....6....6....7..
```

```
             0    5    0    5    0    5    0    5    0    5    0    5    0
      Call switching rate / CPS (last 72 hours)
      * = maximum calls/s    # = average calls/s


Device#show call history stats cps detail

   10:23:27 AM Wednesday Sep 25 2019 UTC




  10
   9
   8
   7
   6
   5
   4
   3
   2
   1
    0....5....1....1....2....2....3....3....4....4....5....5....6
              0    5    0    5    0    5    0    5    0    5    0
      Call switching rate / CPS (last 60 seconds)
      # = calls handled by the module per second




                              11
  10
   9
   8
   7
   6
   5
   4
   3
   2
   1                          **
    0....5....1....1....2....2....3....3....4....4....5....5....6
              0    5    0    5    0    5    0    5    0    5    0
      Call switching rate / CPS  (last 60 minutes)
      * = maximum calls/s    # = average calls/s



     1
  10
   9
   8
   7
   6
   5
   4
   3
   2
```

```
 1 *
  0....5....1....1....2....2....3....3....4....4....5....5....6....6....7..
            0    5    0    5    0    5    0    5    0    5    0    5    0
       Call switching rate / CPS (last 72 hours)
       * = maximum calls/s    # = average calls/s


10:23:27 AM Wednesday Sep 25 2019 UTC




10
 9
 8
 7
 6
 5
 4
 3
 2
 1
  0....5....1....1....2....2....3....3....4....4....5....5....6
            0    5    0    5    0    5    0    5    0    5    0
       Call-leg switching rate (last 60 seconds)
       # = call legs handled by the module per second



                           11
10
 9
 8
 7
 6
 5
 4
 3
 2
 1                         **
  0....5....1....1....2....2....3....3....4....4....5....5....6
            0    5    0    5    0    5    0    5    0    5    0
       Call-leg switching rate (last 60 minutes)
       * = maximum call-legs/s    # = average call-legs/s



   1
10
 9
 8
 7
 6
 5
 4
 3
 2
 1 *
```

```
     0....5....1....1....2....2....3....3....4....4....5....5....6....6....7..
               0    5    0    5    0    5    0    5    0    5    0    5    0
          Call-leg switching rate (last 72 hours)
          * = maximum call-legs/s    # = average call-legs/s


Device#show call history stats cps table

 10:26:50 AM Wednesday Sep 25 2019 UTC


Call switching rate / CPS (last 60 seconds)
Period     Actual     Average
-----------------------------
 1-5           0          0
 6-10          0          0
11-15          0          0
16-20          0          0
21-25          0          0
26-30          0          0
31-35          0          0
36-40          0          0
41-45          0          0
46-50          0          0
51-55          0          0
56-60          0          0


Call switching rate / CPS (last 60 minutes)
Period     Average       Max
-----------------------------
 1-5           0          0
 6-10          0          0
11-15          0          0
16-20          0          0
21-25          0          0
26-30          0          0
31-35          0          1
36-40          0          0
41-45          0          0
46-50          0          0
51-55          0          0
56-60          0          0


Call switching rate / CPS (last 72 hours)
Period     Average       Max
-----------------------------
 1-5           0          1
 6-10          0          0
11-15          0          0
16-20          0          0
21-25          0          0
26-30          0          0
31-35          0          0
36-40          0          0
41-45          0          0
46-50          0          0
51-55          0          0
56-60          0          0
61-65          0          0
66-70          0          0
```

```
71-72             0             0
```

show call history video

To display call history information for signaling connection control protocol (SCCP) video calls, use the **show call history video** command in user EXEC or privileged EXEC mode.

show call history video [[**brief**] [**id** *identifier*] | **compact** [**duration** {**less** | **more**} *seconds*] | **last** *number*]

Syntax Description

brief	(Optional) Displays a truncated version of video call history information.
id *identifier*	(Optional) Displays only the video call history with the specified identifier. Range is a hexadecimal value from 1 to FFFF.
compact	(Optional) Displays a compact version of video call history information.
duration	(Optional) Displays the call history for the specified time duration.
less	Displays the call history for shorter duration calls.
more	Displays the call history for longer duration calls.
seconds	Time, in seconds. The range is from 1 to 2147483647.
last *number*	(Optional) Displays the last calls connected, where the number of calls that appear is defined by the *number*argument. The range is from 1 to100 .

Command Modes

User EXEC (>)
Privileged EXEC (#)

Command History

Cisco IOS Release	Cisco Product	Modification
12.4(4)XC	Cisco Unified CME 4.0	This command was introduced.
12.4(9)T	Cisco Unified CME 4.0	This command was integrated into Cisco IOS Release 12.4(9)T.
12.4(16); 12.4(15)T	Cisco Unified CME 4.0	This command was modified. The Port and BearerChannel display fields were added to the TELE call leg record of the command output.

Examples

The following is sample output from the **show call history video** command with the **compact** option:

```
Router# show call history video compact
      <callID>  A/O FAX T<sec> Codec       type        Peer Address       IP R<ip>:<udp>
Total call-legs: 2
       241      ANS     T17    g729r8      VOIP        P555-0100          192.0.2.0:16926
       242      ORG     T17    g729r8      TELE-VIDEO  P555-0101
```

The table below describes the significant fields shown in the display.

Table 37: show call history video Field Descriptions

Field	Description
callID	Unique identifier for the call leg.
A/O	Call leg was an answer (ANS) or an originator (ORG).
FAX	Fax number for the call leg.
T<sec>	Duration in seconds.
Codec	Codec used for this call leg.
type	Call type for this call leg.
Peer Address	Called or calling number of the remote peer.
IP R<ip>:<udp>	IP address and port number
Total call-legs	Total number of call legs for this call.

Related Commands

Command	Description
show call active video	Displays call information for SCCP video calls in progress.

show call history video record

To display information about incoming and outgoing video calls, use the **s how call history video record**command in privileged EXEC mode.

show call history video record

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.0(5)XK	This command was introduced on the Cisco MC3810.
12.0(7)T	This command was integrated into Cisco IOS Release 12.0(7)T.

Examples

The following example displays information about two video calls:

```
Router# show call history video record
CallId = 4
CalledNumber = 221
CallDuration = 39006 seconds
DisconnectText = remote hangup
SVC: call ID = 8598630
Remote NSAP = 47.0091810000000002F26D4901.00107B09C645.C8
Local NSAP = 47.0091810000000002F26D4901.00107B4832E1.C8
vcd = 414, vpi = 0, vci = 158
SerialPort = Serial0
VideoSlot = 1, VideoPort = 0
CallId = 3
CalledNumber = 221
CallDuration = 557 seconds
DisconnectText = local hangup
SVC: call ID = 8598581
Remote NSAP = 47.0091810000000002F26D4901.00107B09C645.C8
Local NSAP = 47.0091810000000002F26D4901.00107B4832E1.C8
vcd = 364, vpi = 0, vci = 108
SerialPort = Serial0
VideoSlot = 1, VideoPort = 0
```

show call history voice

To display the call history table for voice calls, use the **show call history voice** command in user EXEC or privileged EXEC mode.

show call history voice [**brief** [**id** *identifier*] | **compact** [**duration** {**less** | **more**} *seconds*] | **dest-route-string** *tag* | **id** *identifier* | **last** *number* | **redirect** {**rtpvt** | **tbct**} | **stats**]

Syntax Description

brief	(Optional) Displays a truncated version of the call history table.
id *identifier*	(Optional) Displays only the call with the specified identifier. Range is from 1 to FFFF.
compact	(Optional) Displays a compact version of the call history table.
dest-route-string *tag*	(Optional) Displays only the call with the specified destination route *tag* value. The range is from 1 to 10000.
duration *seconds*	(Optional) Displays history information for calls that are longer or shorter than the value of the specified *seconds* argument. The arguments and keywords are as follows: • **less** --Displays calls shorter than the *seconds* value. • **more** --Displays calls longer than the *seconds* value. • *seconds* --Elapsed time, in seconds. Range is from 1 to 2147483647.
last *number*	(Optional) Displays the last calls connected, where the number of calls that appear is defined by the *number*argument. Range is from 1 to100 .
redirect	(Optional) Displays information about calls that were redirected using Release-to-Pivot (RTPvt) or Two B-Channel Transfer (TBCT). The keywords are as follows: • **rtpvt** --Displays information about RTPvt calls. • **tbct** --Displays information about TBCT calls.
stats	(Optional) Displays information about digital signal processing (DSP) voice quality metrics.

Command Modes

User EXEC (>)
Privileged EXEC (#)

Command History

Release	Modification
11.3(1)T	This command was introduced on the Cisco 3600 series.
12.0(3)XG	Support was added for Voice over Frame Relay (VoFR) on the Cisco 2600 series and Cisco 3600 series.
12.0(4)XJ	This command was modified for store-and-forward fax.

Release	Modification
12.0(4)T	The **brief** keyword was added, and the command was implemented on the Cisco 7200 series.
12.0(5)XK	This command was implemented on the Cisco MC3810.
12.0(7)XK	The **brief** keyword was implemented on the Cisco MC3810.
12.0(7)T	This command was integrated into Cisco IOS Release 12.0(7)T.
12.1(2)T	This command was integrated into Cisco IOS Release 12.1(2)T.
12.1(5)XM	This command was implemented on the Cisco AS5800.
12.1(5)XM2	This command was implemented on the Cisco AS5350 and Cisco AS5400.
12.2(2)XA	The output of this command was modified to indicate whether a specified call has been established using Annex E.
12.2(4)T	This command was integrated into Cisco IOS Release 12.2(4)T.
12.2(2)XB1	This command was implemented on the Cisco AS5850.
12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T. Support was not included for the Cisco AS5350, Cisco AS5400, Cisco AS5800, and Cisco AS5850.
12.2(11)T	Support was added for Cisco AS5350, Cisco AS5400, Cisco AS5800, and Cisco AS5850.
12.2(13)T	The ReleaseSource field was added to the Field Description table, and the **record** keyword was deleted from the command name.
12.3(1)	The **redirect** keyword was added.
12.4(2)T	The LocalHostname display field was added to the VoIP call leg record.
12.4(11)XW	The **stats** keyword was added.
12.4(15)T	The Port and BearerChannel display fields were added to the TELE call leg record of the command output.
12.4(16)	The Port and BearerChannel display fields were added to the TELE call leg record of the command output.
12.4(22)T	Command output was updated to show IPv6 information.
15.3(3)M	This command was modified. The **dest-route-string** keyword was added.
Cisco IOS XE Release 3.10S	This command was integrated into Cisco IOS XE Release 3.10S.

Usage Guidelines

This command displays a call-history table that contains a list of voice calls connected through the router in descending time order. The maximum number of calls contained in the table can be set to a number from 0

to 500 using the **dial-control-mib** command in global configuration mode. The default maximum number of table entries is 50. Each call record is aged out of the table after a configurable number of minutes has elapsed. The timer value is also specified by the **dial-control-mib** command. The default timer value is 15 minutes.

You can display subsets of the call history table by using specific keywords. To display the last calls connected through this router, use the **last** keyword, and define the number of calls to be displayed with the number argument.

To display a truncated version of the call history table, use the **brief** keyword.

Use the **show call active voice redirect** command to review records for calls that implemented RTPvt or TBCT.

When a call is active, you can display its statistics by using the **show call active voice** command.

Use the **show call active voice dest-route-string** command to display only the active voice calls with call routing configured using specified destination-route-string globally and at the dial-peer level.

Examples

The following is sample output from the **show call history voice** command:

```
Router# show call history voice
GENERIC:
SetupTime=104648 ms
Index=1
PeerAddress=55240
PeerSubAddress=
PeerId=2
PeerIfIndex=105
LogicalIfIndex=0
DisconnectCause=10
DisconnectText=normal call clearing.
ConnectTime=104964
DisconectTime=143329
CallDuration=00:06:23
CallOrigin=1
ChargedUnits=0
InfoType=speech
TransmitPackets=37668
TransmitBytes=6157536
ReceivePackets=37717
ReceiveBytes=6158452
VOIP:
ConnectionId[0x4B091A27 0x3EDD0003 0x0 0xFEFD4]
CallID=2
RemoteIPAddress=10.14.82.14
RemoteUDPPort=18202
RoundTripDelay=2 ms
SelectedQoS=best-effort
tx_DtmfRelay=inband-voice
FastConnect=TRUE
SessionProtocol=cisco
SessionTarget=ipv4:10.14.82.14
OnTimeRvPlayout=40
GapFillWithSilence=0 ms
GapFillWithPrediction=0 ms
GapFillWithInterpolation=0 ms
GapFillWithRedundancy=0 ms
HiWaterPlayoutDelay=67 ms
LoWaterPlayoutDelay=67 ms
ReceiveDelay=67 ms
LostPackets=0 ms
```

```
EarlyPackets=0 ms
LatePackets=0 ms
VAD = enabled
CoderTypeRate=g729r8
CodecBytes=20
cvVoIPCallHistoryIcpif=0
SignalingType=cas
Modem passthrough signaling method is nse
Buffer Fill Events = 0
Buffer Drain Events = 0
Percent Packet Loss = 0
Consecutive-packets-lost Events = 0
Corrected packet-loss Events = 0
Last Buffer Drain/Fill Event = 373sec
Time between Buffer Drain/Fills = Min 0sec Max 0sec
GENERIC:
SetupTime=104443 ms
Index=2
PeerAddress=50110
PeerSubAddress=
PeerId=100
PeerIfIndex=104
LogicalIfIndex=10
DisconnectCause=10
DisconnectText=normal call clearing.
ConnectTime=104964
DisconectTime=143330
CallDuration=00:06:23
CallOrigin=2
ChargedUnits=0
InfoType=speech
TransmitPackets=37717
TransmitBytes=5706436
ReceivePackets=37668
ReceiveBytes=6609552
TELE:
ConnectionId=[0x4B091A27 0x3EDD0003 0x0 0xFEFD4]
CallID=3
Port=3/0/0 (3)
BearerChannel=3/0/0.1
TxDuration=375300 ms
VoiceTxDuration=375300 ms
FaxTxDuration=0 ms
CoderTypeRate=g711ulaw
NoiseLevel=-75
ACOMLevel=11
SessionTarget=
ImgPages=0
```

The following example from a Cisco AS5350 router displays a sample of voice call history records showing release source information:

```
Router# show call history voice
Telephony call-legs: 1
SIP call-legs: 0
H323 call-legs: 1
Total call-legs: 2
GENERIC:
SetupTime=85975291 ms
.
.
.
DisconnectCause=10
```

```
DisconnectText=normal call clearing (16)
ConnectTime=85975335
DisconnectTime=85979339
CallDuration=00:00:40
CallOrigin=1
ReleaseSource=1
.
.
.
DisconnectCause=10
DisconnectText=normal call clearing (16)
ConnectTime=85975335
DisconnectTime=85979339
CallDuration=00:00:40
CallOrigin=1
ReleaseSource=1
.
.
.
VOIP:
ConnectionId[0x2868AD84 0x375B11D4 0x8012F7A5 0x74DE971E]
CallID=1
.
.
.
GENERIC:
SetupTime=85975290 ms
.
.
.
DisconnectCause=10
DisconnectText=normal call clearing (16)
ConnectTime=85975336
DisconnectTime=85979340
CallDuration=00:00:40
CallOrigin=2
ReleaseSource=1
.
.
.
TELE:
ConnectionId=[0x2868AD84 0x375B11D4 0x8012F7A5 0x74DE971E]
CallID=2
Port=3/0/0 (2)
BearerChannel=3/0/0.1
```

The following is sample output from the **show call history voice brief** command:

```
Router# show call history voice brief
<ID>: <CallID> <start>hs.<index> +<connect> +<disc> pid:<peer_id> <direction> <addr>
dur hh:mm:ss tx:<packets>/<bytes> rx:<packets>/<bytes> <disc-cause>(<text>)
IP <ip>:<udp> rtt:<time>ms pl:<play>/<gap>ms lost:<lost>/<early>/<late>
delay:<last>/<min>/<max>ms <codec>
media inactive detected:<y/n> media cntrl rcvd:<y/n> timestamp:<time>
MODEMPASS <method> buf:<fills>/<drains> loss <overall%> <multipkt>/<corrected>
last <buf event time>s dur:<Min>/<Max>s
FR <protocol> [int dlci cid] vad:<y/n> dtmf:<y/n> seq:<y/n>
<codec> (payload size)
ATM <protocol> [int vpi/vci cid] vad:<y/n> dtmf:<y/n> seq:<y/n>
<codec> (payload size)
Telephony <int> (callID) [channel_id] tx:<tot>/<voice>/<fax>ms <codec> noise:<lvl>dBm
acom:<lvl>dBm
MODEMRELAY info:<rcvd>/<sent>/<resent> xid:<rcvd>/<sent> total:<rcvd>/<sent>/<drops>
disc:<cause code>
```

```
speeds(bps): local <rx>/<tx> remote <rx>/<tx>
Proxy <ip>:<audio udp>,<video udp>,<tcp0>,<tcp1>,<tcp2>,<tcp3> endpt: <type>/<manf>
bw: <req>/<act> codec: <audio>/<video>
tx: <audio pkts>/<audio bytes>,<video pkts>/<video bytes>,<t120 pkts>/<t120 bytes>
rx: <audio pkts>/<audio bytes>,<video pkts>/<video bytes>,<t120 pkts>/<t120 bytes>
```

The following is sample output from the **show call history voice redirect** command:

```
Router# show call history voice redirect tbct
index=2, xfr=tbct-notify, status=redirect_success, start_time=*00:12:25.981 UTC Mon Mar 1
1993, ctrl name=T1-2/0,  tag=13
index=3, xfr=tbct-notify, status=redirect_success, start_time=*00:12:25.981 UTC Mon Mar 1
1993, ctrl name=T1-2/0,  tag=13
index=4, xfr=tbct-notify, status=redirect_success, start_time=*00:13:07.091 UTC Mon Mar 1
1993, ctrl name=T1-2/0,  tag=12
index=5, xfr=tbct-notify, status=redirect_success, start_time=*00:13:07.091 UTC Mon Mar 1
1993, ctrl name=T1-2/0,  tag=12
Number of call-legs redirected using tbct with notify:4
```

The table below describes the significant fields shown in the **show call history voice redirect tbct** display.

Table 38: show call history voice redirect Field Descriptions

Field	Description
index	Index number of the record in the history file.
xfr	Whether TBCT or TBCT with notify has been invoked.
status	Status of the redirect request.
start_time	Time, in hours, minutes, and seconds when the redirected call began.
ctrl name	Name of the T1 controller where the call originated.
tag	Call tag number that identifies the call.
Number of call-legs redirected using tbct with notify	Total number of call legs that were redirected using TBCT with notify.

Related Commands

Command	Description
dial-control-mib	Set the maximum number of calls contained in the table.
show call active fax	Displays call information for fax transmissions that are in progress.
show call active voice	Displays call information for voice calls that are in progress.
show call history fax	Displays the call history table for fax transmissions.
show dial-peer voice	Displays configuration information for dial peers.
show num-exp	Displays how the number expansions are configured in VoIP.
show voice port	Displays configuration information about a specific voice port.

show call history watermark connected table

To display the last **n** high watermark that is achieved by number of connected call rates per second in various periods, use the **show call history watermark connected table** command. The periods are seconds, minutes, and hours since the last reload. The size of the table is variable and is configurable.

show call history watermark connected table [[**brief**] [**id** *identifier*] | **compact** [**duration** {**less** | **more**} *seconds*] | **last** *number*]

This command has no arguments or keywords.

Command Modes

Privileged EXEC (#)

Cisco IOS Release	Modification
15.3(1)T	This command was introduced.

The following is a sample output in the **show call history watermark connected table** command:

The output displays a tabular format of call rate per second for the last 1 minute, 1 hour, and all time.

```
Device#show call history watermark connected table
Device   01:48:05 AM Thursday Mar 14 2019 UTC
===========================================
Connected Calls
------- The WaterMark Table for Second --------
Value : 0, ts : [Thu, 14 Mar 2019 01:48:01 GMT]
Value : 0, ts : [Thu, 14 Mar 2019 01:48:02 GMT]
Value : 0, ts : [Thu, 14 Mar 2019 01:48:03 GMT]
Value : 0, ts : [Thu, 14 Mar 2019 01:48:04 GMT]
Value : 0, ts : [Thu, 14 Mar 2019 01:48:05 GMT]
------- The WaterMark Table for Minute-------
Value : 0, ts : [Wed, 13 Mar 2019 05:33:06 GMT]
Value : 0, ts : [Wed, 13 Mar 2019 05:33:06 GMT]
Value : 0, ts : [Wed, 13 Mar 2019 05:33:06 GMT]
Value : 0, ts : [Wed, 13 Mar 2019 05:33:06 GMT]
Value : 0, ts : [Wed, 13 Mar 2019 05:33:06 GMT]
------- The WaterMark Table for Hour --------
Value : 0, ts : [Wed, 13 Mar 2019 05:16:05 GMT]
Value : 0, ts : [Wed, 13 Mar 2019 05:16:05 GMT]
Value : 0, ts : [Wed, 13 Mar 2019 05:16:05 GMT]
Value : 1, ts : [Wed, 13 Mar 2019 00:12:05 GMT]
Value : 1, ts : [Wed, 13 Mar 2019 05:16:05 GMT]
------- The WaterMark Table for Alltime------
Value : 1, ts : [Sun, 10 Mar 2019 01:39:05 GMT]
Value : 1, ts : [Sun, 10 Mar 2019 23:06:05 GMT]
Value : 1, ts : [Wed, 13 Mar 2019 00:12:05 GMT]
Value : 1, ts : [Wed, 13 Mar 2019 05:16:05 GMT]
Value : 2, ts : [Sun, 10 Mar 2019 23:57:05 GMT]
Device#
```

Usage Guidelines

This command displays the last n high watermark that is achieved by number of connected call rates per second in various periods. The periods are seconds, minutes, and hours since the last reload.

Related Commands

Command	Description
show call history stats connected	Display connected or active call histogram for 3 periods (Seconds, Minutes, and Hours).
show call history stats connected table	Displays concurrent call table for max and average value of active calls per second.

show call language voice

To display a summary of languages configured and the URLs of the corresponding Tool Command Language (TCL) modules for the languages that are not built-in languages, use the **show call language voice command in**EXEC mode.

show call language voice [*language* | **summary**]

Syntax Description

language	(Optional) Two-character prefix configured with the **call language voice** command in global configuration mode, either for a prefix for a built-in language or one that you have defined; for example, "en" for English or "ru" for Russian.
summary	(Optional) Summary of all the languages configured and the URLs for the TCL modules other than built-in languages.

Command Modes

EXEC (#)

Command History

Release	Modification
12.2(2)T	This command was introduced.

Usage Guidelines

This command is similar to the **show call application voice** command. If a language is built in, the URL listed reads "fixed." If you decide to overwrite the built-in language with your own language, the word "fixed" in the URL column changes to the actual URL where your new application lives.

Examples

The following command displays a summary of the configured languages:

```
Router# show call language voice summary
name       url
sp         fixed
ch         fixed
en         fixed
ru         tftp://dirt/fwarlau/scripts/multilag/ru_translate.tcl
```

The following command displays information about Russian-language configuration:

```
Router# show call language voice ru
ru_translate.tcl
ru_translate.tcl~
singapore.cfg
test.tcl
people% more ru_translate.tcl
# Script Locked by: farmerj
# Script Version: 1.1.0.0
# Script Lock Date: Sept 24 2000
# ca_translate.tcl
#-----------------------------------------------------------------
# Sept 24, 2000 Farmer Joe
#
# Copyright (c) 2000 by Cisco Systems, Inc.
# All rights reserved.
```

```
#-------------------------------------------------------------------
#<snip>...
...set prefix ""
#puts "argc"
#foreach arg $argv {
#puts "$arg"
#    translates $arg
#    puts "\t\t**** $prompt RETURNED"
#}
```

Field descriptions should be self-explanatory.

Related Commands

Command	Description
call language voice	Configures a TCL module.
call language voice load	Loads or reloads a TCL module from the configured URL location.
debug voip ivr	Specifies the type of VoIP IVR debug output that you want to view.
show call application voice	Shows and describes applications.

show call leg

To display event logs and statistics for voice call legs, use the **show call leg**command in privileged EXEC mode.

show call leg {**active** | **history**} [**summary** | [**last** *number* | **leg-id** *leg-id*] [**event-log** | **info**]]

Syntax Description

active	Statistics or event logs for active call legs.
history	Statistics or event logs for terminated call legs.
summary	(Optional) A summary of each call leg.
last *number*	(Optional) Selected number of most recent call legs. Not available with **active** keyword.
leg-id *leg-id*	(Optional) A specific call leg. Output displays event logs or statistics for that call leg.
event-log	(Optional) Event logs for call legs.
info	(Optional) Statistics for call legs.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.3(8)T	This command was introduced.

Usage Guidelines

If you use the **leg-id** keyword, only statistics or event logs for that call leg display. To display event logs with this command, you must enable event logging with the **call leg event-log** command.

Examples

The following is sample output from the **show call leg** command using different keywords:

```
Router# show call leg active summary
G<id>  L<id>     Elog A/O FAX T<sec> Codec       type  Peer Address       IP R<ip>:<udp>
G11DC  L A        Y   ANS     T2     None        TELE  P4085550198
Total call-legs: 1
Router# show call leg active event-log

Event log for call leg ID: A        Connection ID: 11DC
buf_size=4K, log_lvl=INFO
<ctx_id>:<timestamp>:<seq_no>:<severity>:<msg_body>
A:1057277701:71:INFO: Call setup indication received, called = 4085550198,  calling = 52927,
 echo canceller = enable, direct inward dialing
A:1057277701:72:INFO: Dialpeer = 1
A:1057277701:77:INFO: Digit collection
A:1057277701:78:INFO: Call connected using codec None
Total call-legs: 1
Router# show call leg active info

Information for call leg ID: A        Connection ID: 11DC
 GENERIC:
```

```
SetupTime=3012940 ms
Index=1
PeerAddress=4085550198
PeerSubAddress=
PeerId=1
PeerIfIndex=329
LogicalIfIndex=253
ConnectTime=301295
CallDuration=00:00:20
CallState=4
CallOrigin=2
ChargedUnits=0
InfoType=2
TransmitPackets=412
TransmitBytes=98880
ReceivePackets=0
ReceiveBytes=0
TELE:
ConnectionId=[0x632D2CAB 0xACEB11D7 0x80050030 0x96F8006E]
IncomingConnectionId=[0x632D2CAB 0xACEB11D7 0x80050030 0x96F8006E]
TxDuration=20685 ms
VoiceTxDuration=0 ms
FaxTxDuration=0 ms
CoderTypeRate=None
NoiseLevel=-120
ACOMLevel=90
OutSignalLevel=-50
InSignalLevel=-41
InfoActivity=0
ERLLevel=38
EchoCancellerMaxReflector=16685
SessionTarget=
ImgPages=0
CallerName=
CallerIDBlocked=False
OriginalCallingNumber=4085550198
OriginalCallingOctet=0x0
OriginalCalledNumber=52927
OriginalCalledOctet=0xE9
OriginalRedirectCalledNumber=
OriginalRedirectCalledOctet=0xFF
TranslatedCallingNumber=4085550198
TranslatedCallingOctet=0x0
TranslatedCalledNumber=52927
TranslatedCalledOctet=0xE9
TranslatedRedirectCalledNumber=
TranslatedRedirectCalledOctet=0xFF
GwReceivedCalledNumber=52927
GwReceivedCalledOctet3=0xE9
GwReceivedCallingNumber=4085550198
GwReceivedCallingOctet3=0x0
GwReceivedCallingOctet3a=0x81
Total call-legs: 1
```

For a description of the call leg statistics, see the description for the **show call active voice** command.

```
Router# show call leg active leg-id A

Call Information - Connection ID: 11DC , Call Leg ID: A
 GENERIC:
SetupTime=3012940 ms
Index=1
PeerAddress=4085550198
PeerSubAddress=
```

```
PeerId=1
PeerIfIndex=329
LogicalIfIndex=253
ConnectTime=301295
CallDuration=00:00:40
CallState=4
CallOrigin=2
ChargedUnits=0
InfoType=2
TransmitPackets=824
TransmitBytes=197760
ReceivePackets=0
ReceiveBytes=0
TELE:
ConnectionId=[0x632D2CAB 0xACEB11D7 0x80050030 0x96F8006E]
IncomingConnectionId=[0x632D2CAB 0xACEB11D7 0x80050030 0x96F8006E]
TxDuration=20685 ms
VoiceTxDuration=0 ms
FaxTxDuration=0 ms
CoderTypeRate=None
NoiseLevel=-120
ACOMLevel=90
OutSignalLevel=-50
InSignalLevel=-41
InfoActivity=0
ERLLevel=38
EchoCancellerMaxReflector=16685
SessionTarget=
ImgPages=0
CallerName=
CallerIDBlocked=False
OriginalCallingNumber=4085550198
OriginalCallingOctet=0x0
OriginalCalledNumber=52927
OriginalCalledOctet=0xE9
OriginalRedirectCalledNumber=
OriginalRedirectCalledOctet=0xFF
TranslatedCallingNumber=4085550198
TranslatedCallingOctet=0x0
TranslatedCalledNumber=52927
TranslatedCalledOctet=0xE9
TranslatedRedirectCalledNumber=
TranslatedRedirectCalledOctet=0xFF
GwReceivedCalledNumber=52927
GwReceivedCalledOctet3=0xE9
GwReceivedCallingNumber=4085550198
GwReceivedCallingOctet3=0x0
GwReceivedCallingOctet3a=0x81
Call Event Log - Connection ID: 11DC , Call Leg ID: A
buf_size=4K, log_lvl=INFO
<ctx_id>:<timestamp>:<seq_no>:<severity>:<msg_body>
A:1057277701:71:INFO: Call setup indication received, called = 4085550198,  calling = 52927,
 echo canceller = enable, direct inward dialing
A:1057277701:72:INFO: Dialpeer = 1
A:1057277701:77:INFO: Digit collection
A:1057277701:78:INFO: Call connected using codec None
Call-leg found: 1
Router# show call leg active leg-id A event-log

Call Event Log - Connection ID: 11DC , Call Leg ID: A
buf_size=4K, log_lvl=INFO
<ctx_id>:<timestamp>:<seq_no>:<severity>:<msg_body>
A:1057277701:71:INFO: Call setup indication received, called = 4085550198,  calling = 52927,
 echo canceller = enable, direct inward dialing
```

```
A:1057277701:72:INFO: Dialpeer = 1
A:1057277701:77:INFO: Digit collection
A:1057277701:78:INFO: Call connected using codec None
Call-leg found: 1
Router# show call leg history summary

G<id>  L<id>     Elog A/O FAX T<sec> Codec       type  Peer Address       IP R<ip>:<udp>
disc-cause
G11DB  L 7        Y   ANS     T24    None        TELE  P4085550198 D10
G11DC  L A        Y   ANS     T159   None        TELE  P4085550198 D10
Total call-legs: 2
Router# show call leg history last 1
Call Information - Connection ID: 11DC , Call Leg ID: A
GENERIC:
SetupTime=3012940 ms
Index=4
PeerAddress=4085550198
PeerSubAddress=
PeerId=1
PeerIfIndex=329
LogicalIfIndex=253
DisconnectCause=10
DisconnectText=normal call clearing (16)
ConnectTime=301295
DisconnectTime=317235
CallDuration=00:02:39
CallOrigin=2
ReleaseSource=1
ChargedUnits=0
InfoType=speech
TransmitPackets=2940
TransmitBytes=705600
ReceivePackets=0
ReceiveBytes=0
TELE:
ConnectionId=[0x632D2CAB 0xACEB11D7 0x80050030 0x96F8006E]
IncomingConnectionId=[0x632D2CAB 0xACEB11D7 0x80050030 0x96F8006E]
TxDuration=20685 ms
VoiceTxDuration=0 ms
FaxTxDuration=0 ms
CoderTypeRate=None
NoiseLevel=-120
ACOMLevel=90
SessionTarget=
ImgPages=0
CallerName=
CallerIDBlocked=False
OriginalCallingNumber=4085550198
OriginalCallingOctet=0x0
OriginalCalledNumber=52927
OriginalCalledOctet=0xE9
OriginalRedirectCalledNumber=
OriginalRedirectCalledOctet=0xFF
TranslatedCallingNumber=4085550198
TranslatedCallingOctet=0x0
TranslatedCalledNumber=52927
TranslatedCalledOctet=0xE9
TranslatedRedirectCalledNumber=
TranslatedRedirectCalledOctet=0xFF
GwReceivedCalledNumber=52927
GwReceivedCalledOctet3=0xE9
GwReceivedCallingNumber=4085550198
GwReceivedCallingOctet3=0x0
GwReceivedCallingOctet3a=0x81
```

```
Call Event Log - Connection ID: 11DC , Call Leg ID: A
buf_size=4K, log_lvl=INFO
<ctx_id>:<timestamp>:<seq_no>:<severity>:<msg_body>
A:1057277701:71:INFO: Call setup indication received, called = 4085550198,  calling = 52927,
 echo canceller = enable, direct inward dialing
A:1057277701:72:INFO: Dialpeer = 1
A:1057277701:77:INFO: Digit collection
A:1057277701:78:INFO: Call connected using codec None
A:1057277860:150:INFO: Inform application call disconnected (cause = normal call clearing
(16))
A:1057277860:154:INFO: Call disconnected (cause = normal call clearing (16))
A:1057277860:155:INFO: Call released
Total call-legs: 1
Total call-legs with event log: 1
Router# show call leg history leg-id A event-log

Call Event Log - Connection ID: 11DC , Call Leg ID: A
buf_size=4K, log_lvl=INFO
<ctx_id>:<timestamp>:<seq_no>:<severity>:<msg_body>
A:1057277701:71:INFO: Call setup indication received, called = 4085550198,  calling = 52927,
 echo canceller = enable, direct inward dialing
A:1057277701:72:INFO: Dialpeer = 1
A:1057277701:77:INFO: Digit collection
A:1057277701:78:INFO: Call connected using codec None
A:1057277860:150:INFO: Inform application call disconnected (cause = normal call clearing
(16))
A:1057277860:154:INFO: Call disconnected (cause = normal call clearing (16))
A:1057277860:155:INFO: Call released
Call-leg matched ID found: 1
Call-legs matched ID with event log: 1
```

Field descriptions should be self-explanatory.

Related Commands

Command	Description
call leg event-log	Enables event logging for voice, fax, and modem call legs.
call leg event-log dump ftp	Enables the voice gateway to write the contents of the call-leg event log buffer to an external file.
call leg event-log error-only	Restricts event logging to error events only for voice call legs.
call leg event-log max-buffer-size	Sets the maximum size of the event log buffer for each call leg.
call leg history event-log save-exception-only	Saves to history only event logs for call legs that had at least one error.
monitor call leg event-log	Displays the event log for an active call leg in real-time.

show call media forking

To display currently active media forking sessions, use the **show call media forking** command in user EXEC or privileged EXEC mode.

show call media forking

Syntax Description

This command has no arguments or keywords.

Command Modes

User EXEC (>)
Privileged EXEC (#)

Command History

Release	Modification
15.2(2)T	This command was introduced.

Usage Guidelines

Use this command to verify that media forking was successful for relevant anchor legs.

Examples

The following example is a sample output from the s**how call media forking** command..

```
Router# show call media forking
Warning: Output may be truncated if sessions are added/removed concurrently!
Session Call n/f Destination (port address)
7 6 far 1234 1.5.35.254
8 6 near 5678 1.5.35.254
```

The table below describes the fields that are displayed in the output.

Field	Description
Session	Session Identifier.
Call	Call Leg identifier in hexadecimal. It must match the Call ID from the show call leg active command.
n/f	Direction (Near End or Far End) of the voice stream that was forked.
Destination (port address)	Destination for the forked packets. It consists of the folllowing: • RTP Port • IP Address

show callmon

To display call monitor information, use the **show callmon** command in user EXEC or privileged EXEC mode.

show callmon {**call** | **gcid** | **subscription** | **trace** {**all** | **event** {**all** | **call** | **connection**} | **exec** | **server** | **subscription** | **trigger**}}

Syntax Description

call	Displays the active call monitor calls.
gcid	Displays the active global call ID information.
subscription	Displays the subscription information.
trace	Displays the trace information.
all	Displays all types of traces based on time.
event	Displays the event trace information. • **all** --Displays all event traces. • **call** --Displays event traces related to a call. • **connection** --Displays the event traces related to a connection.
exec	Displays all critical execution traces.
server	Displays all session server up or down traces.
subscription	Displays all subscription traces.
trigger	Displays the entire trigger structure by index.

Command Modes

User EXEC (>)
Privileged EXEC (#))

Command History

Release	Modification
12.4(22)T	This command was introduced.

Examples

The following sample output from the **show callmon call** command shows active call monitor calls:

```
Router# show callmon call
 line dn     sub_id   number of call instance
6401,     1
      callID 2038(19D7),  *cg = 6401, cd = 6601
6601,     1
      callID 2039(19D7),  cg = 6401, *cd = 6601
```

The table below describes the significant fields shown in the display.

Table 39: show callmon call Field Descriptions

Field	Description
dn	Directory number.
number of call	Number of call instances.
instance	Contents of the call instance.

The following sample output from the **show callmon gcid** command shows the active global call ID information:

```
Router# show callmon gcid
 GCID                                callIDs(active_entry_id)
AE48ECBC-D89311DB-87FC996E-115FF692
 isConfGcid:FALSE        gcid_conf:00000000-00000000-00000000-00000000
, 2038(19D7), 2039(19D7)
```

The table below describes the significant fields shown in the display.

Table 40: show callmon gcid Field Descriptions

Field	Description
GCID	Global call ID.
CallIDs	Active call IDs.

Related Commands

Command	Description
callmonitor	Enables call monitoring messaging functionality on a SIP endpoint in a VoIP network.

show call prompt-mem-usage

To display the amount of memory used by prompts, use the **show call prompt-mem-usage**command in privileged EXEC mode.

show call prompt-mem-usage [**detail**]

Syntax Description

detail	(Optional) Displays details about memory usage and names of tones used.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.2(15)T	This command was introduced.
12.3(7)T	The **detail** keyword was added.

Usage Guidelines

Use this command to display the number of prompts loaded into the gateway, the amount of memory used by the prompts, the number of prompts currently being played, and the status of prompt loads.

For calls transferred by a Cisco CallManager Express (Cisco CME) system, the ringback tone generation for commit-at-alerting uses an interactive voice response (IVR) prompt playback mechanism. Ringback tone is played to the transferred party by the Cisco CME system associated with the transferring party.

The system automatically generates tone prompts as needed on the basis of the network-locale setting made in the Cisco CME system.

Examples

The following sample output shows details about the memory usage of the prompts that are used.

```
Router# show call prompt-mem-usage
Prompt memory usage:
             config'd      wait    active      free     mc total    ms total
    file(s)      0200      0010      0001     00189        00011       00002
    memory   02097152  00081259  00055536  01960357     00136795
 Prompt load counts: (counters reset 0)
    success 11(1st try) 0(2nd try), failure 0
 Other mem block usage:
            mcDynamic   mcReader
    gauge       00001      00001
Number of prompts playing: 1
Number of start delays   : 0
MCs in the ivr MC sharing table
================================
Media Content: NoPrompt (0x83C64554)
  URL:
  cid=0, status=MC_READY size=24184 coding=g711ulaw refCount=0
Media Content: tone://GB_g729_tone_ringback (0x83266EC8)
  URL: tone://GB_g729_tone_ringback
```

The table below describes the significant fields shown in the display.

Table 41: show call prompt-mem-usage Field Descriptions

Field	Description
file(s)	Number of prompts in different queues.
file(s) - config'd	Maximum number of configured prompts that can be simultaneously available in memory. In the sample output, the value of 200 in this field means that loading the 201st prompt results in the oldest prompts being removed.
file(s) -wait	Number of prompts in the wait queue that are not being used in any call and are ready to be deleted when there is no space for a new prompt. This field lists older prompts that can be deleted.
file(s) - active	Number of prompts that are being used in active calls. These prompts cannot be deleted.
file(s) - free	Number of prompts that can be loaded without deleting any prompt from the wait queue. This is the number of configured prompts (listed under config'd) minus the total number of prompts in the wait and active states.
file(s) - mc total	Total number of prompts in the wait and active states.
ms total	Number of media streams that are currently active. One media stream is used for playing INBOX prompts. A prompt is considered an INBOX prompt if its URL is either flash:, http:, ram:, or tftp:.
memory	Displays the memory used by prompts, in bytes.
memory - config'd	Maximum amount of memory configured to be available for prompts.
memory - wait	Total amount of memory used by prompts in the wait list.
memory - active	Total amount of memory used by prompts in the active list.
memory - free	Amount of available memory. This is the amount of configured prompts (listed under config'd) memory minus the total amount of memory used by the prompts in the wait and active lists.
memory - mc total	Total amount of memory used by prompts in the wait and active lists.
Prompt load counts	Number of successful attempts to load a prompt on the first try and on the second try, and the number of attempts to load a prompt that failed.
mcDynamic	Number of dynamic element queues that are active. A dynamic element queue is a list of prompts that are played together.
mcReader	Number of mcReaders that are active. An mcReader is used for playing one mcDynamic queue of prompts. An mcReader is used only if the mcDynamic contains prompts that are associated with one of the following types of URL: flash:, http:, ram:, or tftp:.
Number of prompts playing	Number of prompts that are currently playing.
Number of start delays	Number of times that prompts failed to start and have subsequently restarted.

Field	Description
MCs in the ivr MC sharing table	The fields below this line of text refer to each media content (prompt) currently cached in memory. In the sample output, the only cached prompt is the built-in default prompt named "NoPrompt."
Media Content	Name of the prompt, which is derived from the audio file URL (the characters after the last "/" in the URL). The address in parentheses is the memory location of the prompt.
URL	Location of the file for the prompt that is playing. In the case of the default prompt, NoPrompt, no URL is given.
cid	Call identification number of the call that initiated the loading of the prompt.
status	Status of the media content. The following values are possible: • MC_NOT_READY--Initial status for media content. When the media content is successfully loaded, the status will change to MC_READY. • MC_READY--Media content is loaded into memory and ready for use. • MC_LOAD_FAIL--Media content failed to load.
size	Size of the media content, in bytes.
coding	Type of encoding used by the media content.
refCount=0	Number of calls to which this media content is currently being streamed.

show call resource voice stats

To display resource statistics for an H.323 gateway, use the show call resource voice stats command in privileged EXEC mode.

show call resource voice stats [**ds0** | **dsp**]

Syntax Description

ds0	(Optional) Specifies the voice digital signal level zero (DS0) resource statistics information.
dsp	(Optional) Specifies the voice digital signal processor (DSP) resource statistics information.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.0(5)T	This command was introduced.
12.1(5)XM2	This command was integrated into Cisco IOS Release 12.1(5)XM2
12.2(4)T	This command was integrated into Cisco IOS Release 12.2(4)T.
12.2(2)XB1	This command was integrated into Cisco IOS Release into 12.2(2)XB1.
12.2(8)T	This command was modified. Support for the Cisco AS5300,Cisco AS5350, Cisco AS5400, Cisco AS5800, and Cisco AS5850 series routers is not included in this release.
12.4(22)T	This command was modified. The **ds0** and **dsp** keywords were added.

Usage Guidelines

The **show call resource voice stats** command displays the H.323 resources that are monitored when the **resource threshold** command is used to configure resource threshold reporting.

Examples

The following is sample output from the show call resource voice stats command, which shows the resource statistics for an H.323 gateway:

```
Router# show call resource voice stats
Resource Monitor -  Dial-up Resource Statistics Information:
DSP Statistics:
Utilization: 0 percent
Total channels: 48
Inuse channels: 0
Disabled channels 0:
Pending channels: 0
Free channels: 48
DS0 Statistics:
Total channels: 0
Addressable channels: 0
Inuse channels: 0
Disabled channels: 0
Free channels: 0
```

The table below describes significant fields shown in this output.

Table 42: show call resource voice stats Field Descriptions

Statistic	Definition
Total channels	Number of channels physically configured for the resource.
Inuse channels	Number of addressable channels that are in use. This value includes all channels that either have active calls or have been reserved for testing.
Disabled channels	Number of addressable channels that are physically down or that have been disabled administratively with the **shutdown** or **busyout** command.
Pending channels	Number of addressable channels that are pending in loadware download.
Free channels	Number of addressable channels that are free.
Addressable channels	Number of channels that can be used for a specific type of dialup service, such as H.323, which includes all the DS0 resources that have been associated with a voice plain old telephone service (POTS) dial plan profile.

Related Commands

Command	Description
resource threshold	Configures a gateway to report H.323 resource availability to the gatekeeper of the gateway.
show call resource voice threshold	Displays the threshold configuration settings and status for an H.323 gateway.

show call resource voice threshold

To display the threshold configuration settings and status for an H.323 gateway, use the **show call resource voice threshold** command in privileged EXEC mode.

show call resource voice threshold [**ds0** | **dsp**]

Syntax Description

ds0	(Optional) Specifies the voice digital signal level zero (DS0) resource statistics information.
dsp	(Optional) Specifies the voice digital signal processor (DSP) resource statistics information.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.0(5)T	This command was introduced.
12.1(5)XM2	This command was integrated into Cisco IOS Release 12.1(5)XM2
12.2(2)XB1	This command was integrated into Cisco IOS Release into 12.2(2)XB1.
12.4(22)T	This command was modified. The **ds0** and **dsp** keywords were added.

Usage Guidelines

The **show call resource voice threshold** command displays the H.323 resource thresholds that are configured with the **resource threshold** command.

Examples

The following is sample output from the show call resource voice threshold command, which shows the resource threshold settings and status for an H.323 gateway:

```
Router# show call resource voice threshold
Resource Monitor -  Dial-up Resource Threshold Information:
DS0 Threshold:
Client Type: h323
High Water Mark: 70
Low Water Mark: 60
Threshold State: init
DSP Threshold:
Client Type: h323
High Water Mark: 70
Low Water Mark: 60
Threshold State: low_threshold_hit
```

The table below describes the significant fields shown in the display.

Table 43: show call resource voice threshold Field Descriptions

Field	Description
High Water Mark	Resource-utilization level that triggers a message indicating that H.323 resource use is high. The range is 1 to 100. A value of 100 indicates that the resource is unavailable.The default is 90.
Low Water Mark	Resource-utilization level that triggers a message indicating that H.323 resource use has dropped below the high-usage level. The range is 1 to 100. The default is 90.

Related Commands

Command	Description
resource threshold	Configures a gateway to report H.323 resource availability to the gatekeeper of the gateway.
show call resource voice stats	Displays resource statistics for an H.323 gateway.

show call rsvp-sync conf

To display the configuration settings for Resource Reservation Protocol (RSVP) synchronization, use the **show call rsvp-sync conf**command in privileged EXEC mode.

show call rsvp-sync conf

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.1(3)XI1	This command was introduced on the Cisco 2600 series, Cisco 3600 series, Cisco 7200, Cisco MC3810, Cisco AS5300, and Cisco AS5800.
12.1(5)T	This command was integrated into Cisco IOS Release 12.1(5)T.
12.2(2)XB1	This command was implemented on the Cisco AS5850.
12.2(8)T	Support for the Cisco AS5300,Cisco AS5350, Cisco AS5400, Cisco AS5800, and Cisco AS5850 is not included in this release.
12.2(11)T	This command is supported on the Cisco AS5300, Cisco AS5350, Cisco AS5400, Cisco AS5800, and Cisco AS5850 in this release.

Examples

The following example shows sample output from this command:

```
Router# show call rsvp-sync conf
VoIP QoS: RSVP/Voice Signaling Synchronization config:
Overture Synchronization is ON
Reservation Timer is set to 10 seconds
```

The table below describes significant fields shown in this output.

Table 44: show call rsvp-sync conf Field Descriptions

Field	Description
Overture Synchronization is ON	Indicates whether RSVP synchronization is enabled.
Reservation Timer is set to xx seconds	Number of seconds for which the RSVP reservation timer is configured.

Related Commands

Command	Description
call rsvp -sync	Enables synchronization between RSVP and the H.323 voice signaling protocol.

Command	Description
call rsvp -sync resv-timer	Sets the timer for RSVP reservation setup.
debug call rsvp -sync events	Displays the events that occur during RSVP synchronization.
show call rsvp -sync stats	Displays statistics for calls that attempted RSVP reservation.

show call rsvp-sync stats

To display statistics for calls that attempted Resource Reservation Protocol (RSVP) reservation, use the **show call rsvp-sync stats** command in privileged EXEC mode.

show call rsvp-sync stats

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.1(3)XI1	This command was introduced.
12.1(5)T	This command was integrated into Cisco IOS Release 12.1(5)T.
12.2(2)XB1	This command was implemented on the Cisco AS5850.
12.2(11)T	This command was integrated into Cisco IOS Release 12.2(11)T.

Examples

The following example shows sample output from this command:

```
Router# show call rsvp-sync stats
VoIP QoS:Statistics Information:
Number of calls for which QoS was initiated   : 18478
Number of calls for which QoS was torn down   : 18478
Number of calls for which Reservation Success was notified : 0
Total Number of PATH Errors encountered : 0
Total Number of RESV Errors encountered : 0
Total Number of Reservation Timeouts encountered : 0
```

The table below describes significant fields shown in this output.

Table 45: show call rsvp-sync stats Field Descriptions

Field	Description
Number of calls for which QoS was initiated	Number of calls for which RSVP setup was attempted.
Number of calls for which QoS was torn down	Number of calls for which an established RSVP reservation was released.
Number of calls for which Reservation Success was notified	Number of calls for which an RSVP reservation was successfully established.
Total Number of PATH Errors encountered	Number of path errors that occurred.
Total Number of RESV Errors encountered	Number of reservation errors that occurred.

Field	Description
Total Number of Reservation Timeouts encountered	Number of calls in which the reservation setup was not complete before the reservation timer expired.

Related Commands

Command	Description
call rsvp -sync	Enables synchronization between RSVP and the H.323 voice signaling protocol.
call rsvp -sync resv-timer	Sets the timer for RSVP reservation setup.
debug call rsvp -sync events	Displays the events that occur during RSVP synchronization.
show call rsvp -sync conf	Displays the RSVP synchronization configuration.

show call spike status

To display the configured call spike threshold and statistics for incoming calls, use the **show call spike status** command in privileged EXEC mode.

show call spike status [**dial-peer** *tag*]

Syntax Description

dial-peer	(Optional) Displays configuration information for a dial peer.
tag	(Optional) Specifies the dial peer identifying number. Range is from 1 to 2147483647.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.2(2)XA	This command was introduced.
12.2(4)T	This command was integrated into Cisco IOS Release 12.2(4)T. This command was not supported on the Cisco AS5300, Cisco AS5350, and Cisco AS5400 in this release.
12.2(2)XB1	This command was implemented on the Cisco AS5850.
12.2(4)XM	This command was implemented on the Cisco 1750 and Cisco 1751. This command was not supported on any other platforms in this release.
12.2(8)T	This command was implemented on the Cisco 7200 series. Support for the Cisco AS5300, Cisco AS5350, Cisco AS5400, and Cisco AS5850 was not included in this release.
12.2(11)T	Support for the Cisco AS5300, Cisco AS5350, Cisco AS5400, and Cisco AS5850 was added in this release.
15.1(3)T	This command was modified. The output fields of the command were modified to include the output at the dial peer level.

Examples

The following is sample output from this command:

```
Router# show call spike status
 Call Spiking:Configured
 Call spiking :NOT TRIGGERED
 total call count in sliding window ::20
```

The table below describes the significant fields shown in the display.

Table 46: show call spike status Field Descriptions

Field	Description
Call Spiking	Current enabled state of call spiking.
Call Spiking	Details if the call spiking limit has been triggered.

Field	Description
total call count in sliding window	Number of calls during the spiking interval.

```
Router# show call spike status dial-peer 400
TAG         CONFIG    SPIKED TOTAL REJECTED CALLS    REJECTED CALLS
400         YES       NO        4                        0
```

The table below describes the significant fields shown in the display.

Table 47: show call spike status (dial peer) Field Descriptions

Field	Description
TAG	Dial peer tag.
CONFIG	Displays if the **call spike** command has been configured.
SPIKED	Details if the call spiking limit has been triggered.
TOTAL REJECTED CALLS	Displays the number of calls rejected due to a call spike in the dial peer.
REJECTED CALLS	Displays the number of calls rejected when the call spike was triggered until the call spike control was released.

Related Commands

Command	Description
call spike	Configures the limit for the number of incoming calls in a short period of time.

show call threshold

To display enabled triggers, current values for configured triggers, and the number of application programming interface (API) calls that were made to global and interface resources, use the **show call threshold** command in privileged EXEC mode.

show call threshold {**config** | **status** [**unavailable**] | **stats**}

Syntax Description

config	Displays the current threshold configuration.
status	Displays the status of all configured triggers and whether or not the CPU is available.
unavailable	(Optional) Displays the status for all unavailable resources.
stats	Displays statistics for API calls; that is, the resource-based measurement.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.2(2)XA	This command was introduced.
12.2(4)T	This command was integrated into Cisco IOS Release 12.2(4)T. This command is not supported on the Cisco AS5300, Cisco AS5350, and Cisco AS5400 platforms in this release.
12.2(2)XB1	This command was implemented on the Cisco AS5850.
12.2(4)XM	This command was implemented on the Cisco 1750 and Cisco 1751. This command is not supported on any other platforms in this release.
12.2(8)T	This command was implemented on the Cisco 7200 series. Support for the Cisco AS5300, Cisco AS5350, Cisco AS5400, and Cisco AS5850 is not included in this release.
12.2(11)T	This command was implemented on the Cisco AS5300, Cisco AS5350, Cisco AS5400, and Cisco AS5850.
15.2(2)T	This command was modified. The output was modified to display the configured bandwidth threshold, bandwidth availability, and call admission control statistics.

Examples

The following is sample output from the **show call threshold config** command:

```
Router# show call threshold config

Some resource polling interval:
  CPU_AVG interval: 60
  Memory interval:  5
IF              Type            Value   Low     High    Enable
-----           ----            -----   ----    ----    ------
Serial3/1:23    int-calls       0       107     107     N/A
N/A             cpu-avg         0        70      90     busy&treat
```

The following is sample output from the **show call threshold status** command:

```
Router# show call threshold status

Status  IF              Type            Value   Low     High    Enable
------  ---             ------          ----    ----    ----    -----
Avail   N/A             total-calls     0       5       5000    busyout
Avail   N/A             cpu-avg         0       5       65      busyout
```

The following is sample output from the **show call threshold status unavailable** command:

```
Router# show call threshold status unavailable

Unavailable configured resources at the current time:
IF              Type            Value   Low     High    Enable
----            -----           -----   ----    ----    -----
```

The following is sample output from the **show call threshold stats** command:

```
Router# show call threshold stats

Total resource check: 0
 successful: 0
 failed:   0
```

The table below describes significant fields shown in this output.

Table 48: show call threshold Field Descriptions

Field	Description
CPU_AVG interval	Interval of configured trigger CPU_AVG.
Memory interval	Interval of configured trigger Memory.
IF	Interface type and number.
Type	Type of resource.
Value	Value of a call that is to be matched against low and high thresholds.
Low	Low threshold.
High	High threshold.
Enable	Shows if busyout and the **call treatment** command are enabled.

Related Commands

Command	Description
call threshold	Enables a resource and defines associated parameters.
call threshold poll-interval	Enables a polling interval threshold for CPU or memory.
clear call threshold	Clears enabled triggers and their associated parameters.

show call treatment

To display the call-treatment configuration and statistics for handling the calls on the basis of resource availability, use the **show call treatment** command in privileged EXEC mode.

show call treatment {**config** | **stats**}

Syntax Description

config	Displays the call treatment configuration.
stats	Displays statistics for handling the calls on the basis of resource availability.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.2(2)XA	This command was introduced.
12.2(4)T	This command was integrated into Cisco IOS Release 12.2(4)T. This command was not supported on the Cisco AS5300, Cisco AS5350, and Cisco AS5400 in this release.
12.2(2)XB1	This command was implemented on the Cisco AS5850.
12.2(4)XM	This command was implemented on the Cisco 1750 and Cisco 1751. This command was not supported on any other platforms in this release.
12.2(8)T	This command was implemented on the Cisco 7200 series. Support for the Cisco AS5300, Cisco AS5350, Cisco AS5400, and Cisco AS5850 is not included in this release.
12.2(11)T	This command is supported on the Cisco AS5300, Cisco AS5350, Cisco AS5400, and Cisco AS5850 in this release.

Examples

The following is sample output from thiscommand:

```
Router# show call treatment config

Call Treatment Config
---------------------
Call treatment is OFF.
Call treatment action is: Reject
Call treatment disconnect cause is: no-resource
Call treatment ISDN reject cause-code is: 41
```

The table below describes significant fields shown in this output.

Table 49: show call treatment config Field Descriptions

Field	Description
Call treatment is:	State of call treatment, either ON or OFF.

Field	Description
Call treatment action is:	Action trigger assigned for call treatment.
Call treatment disconnect cause is:	Reason for disconnect.
Call treatment ISDN reject cause-code is:	Reject code number assigned.

The following is sample output from the **show call treatment**command:

```
Router# show call treatment stats
Call Treatment Statistics
-------------------------
Total Calls by call treatment: 0
Calls accepted by call treatment: 0
Calls rejected by call treatment: 0
Reason          Num. of calls rejected
------          ----------------------
cpu-5sec:       0
cpu-avg:        0
total-mem:      0
io-mem:         0
proc-mem:       0
total-calls:    0
```

The table below describes significant fields shown in this output.

Table 50: show call treatment stats Field Descriptions

Field	Description
Total Calls by call treatment:	Number of calls received and treated.
Calls accepted by call treatment:	Calls that passed treatment parameters.
Calls rejected by call treatment:	Calls that failed treatment parameters.
cpu-5sec	Number of calls rejected for failing the cpu-5sec parameter.
cpu-avg	Number of calls rejected for failing the cpu-avg parameter.
total-mem	Number of calls rejected for failing the total-mem parameter.
io-mem	Number of calls rejected for failing the io-mem parameter.
proc-mem	Number of calls rejected for failing the proc-mem parameter.
total-calls	Number of calls rejected for failing the total-calls parameter.

Related Commands

Command	Description
call treatment on	Enables call treatment to process calls when local resources are unavailable.
call treatment action	Configures the action that the router takes when local resources are unavailable.

Command	Description
call treatment cause-code	Specifies the reason for the disconnection to the caller when local resources are unavailable.
call treatment isdn-reject	Specifies the rejection cause-code for ISDN calls when local resources are unavailable.
clear call treatment stats	Clears the call-treatment statistics.

show call-router routes

To display the routes cached in the current border element (BE), use the show call-router routes in EXEC mode.

show call-router routes [**static** | **dynamic** | **all**]

Syntax Description

static	Descriptors provisioned on the border element.
dynamic	Dynamically learned descriptors.
all	Both static and dynamic descriptors.

Command Default

All

Command Modes

EXEC (#)

Command History

Release	Modification
12.2(2)XA	This command was introduced.
12.2(4)T	This command was integrated into Cisco IOS Release 12.2(4)T.
12.2(2)XB1	This command was implemented on the Cisco AS5850.
12.2(11)T	This command was integrated into Cisco IOS Release 12.2(11)T.

Examples

The following example is sample output from this command.

```
Router# show call-router routes
Static Routes:
==============
  DescriptorID= 6561676C650000000000000000000000A
  lastChanged = 19930301063311
   IP addr         :port       Prefix
   172.18.195.64   :2099       5553122
Dynamic Routes:
===============
  DescriptorID= 506174726F6E6F757300000000000002
  lastChanged = 19930228190012
   IP addr         :port       Prefix
   172.18.195.65   :2099       310
  DescriptorID= 506174726F6E6F757300000000000003
  lastChanged = 19930228190012
   IP addr         :port       Prefix
   172.18.195.65   :2099       555301
  DescriptorID= 506174726F6E6F757300000000000004
  lastChanged = 19930228190012
   IP addr         :port       Prefix
   172.18.195.65   :2099       555302
DescriptorID= 506174726F6E6F757300000000000005
  lastChanged = 19930228190012
```

```
 IP addr         :port       Prefix
 172.18.195.65   :2099       818
DescriptorID= 506174726F6E6F757300000000000001
lastChanged = 19930228190012
 IP addr         :port       Prefix
 172.18.195.65   :2099       1005
```

Field descriptions should be self-explanatory.

Related Commands

Command	Description
show call-router active	Displays active call information for a voice call in progress.
show call-router history	Displays the VoIP call-history table.
show call-router status	Displays the Annex G BE status.
show dial-peer voice	Displays configuration information for dial peers.
show num-exp	Displays how the number expansions are configured in VoIP.
show voice port	Displays configuration information about a specific voice port.

show call-router status

To display the Annex G border element status, use the **show call-router status**command in user EXEC mode.

show call-router status [**neighbors**]

Syntax Description

neighbors	(Optional) Displays the neighbor border element status.

Command Modes

User EXEC (#)

Command History

Release	Modification
12.2(2)XA	This command was introduced.
12.2(4)T	This command was integrated into Cisco IOS Release 12.2(4)T.
12.2(2)XB1	This command was implemented on the Cisco AS5850.
12.2(11)T	This command was integrated into Cisco IOS Release 12.2(11)T and modified to add the **neighbors**keyword.

Examples

The following example displays the Annex G border element status. Note that the example shows the status for two neighbors.:

```
Router# show call-router status neighbors
ANNEX-G CALL ROUTER STATUS:
  ===========================
    Border Element ID Tag   : Celine
    Domain Name             : Celine-Domain
    Border Element State    : UP
    Border Element Local IP : 172.18.193.31:2099
    Advertise Policy        : STATIC descriptors
    Hopcount Value          : 7
    Descriptor TTL          : 3180
    Access Policy           : Neighbors only
    Current Active Calls    : 0
    Current Calls in Cache  : 0
    Cumulative Active Calls : 0
    Usage Ind Messages Sent : 0
    Usage Ind Cfm Rcvd      : 0
    IRRs Received           : 0
    DRQs Received           : 0
    Usage Ind Send Retrys   : 0
  NEIGHBOR INFORMATION:
  =====================
    Local Neighbor ID : (none)
    Remote Element ID : (unknown)
    Remote Domain ID  : (unknown)
    IP Addr           : 1.2.3.4:2099
    Status            : DOWN
    Caching           : OFF
    Query Interval    : 30 MIN (querying disabled)
    Usage Indications :
```

```
  Current Active Calls : 0
  Retry Period         : 600 SEC
  Retry Window         : 3600 MIN
Service Relationship Status: ACTIVE
  Inbound Service Relationship  : DOWN
    Service ID     : (none)
    TTL            : 1200 SEC
  Outbound Service Relationship : DOWN
    Service ID     : (none)
    TTL            : (none)
    Retry interval : 120 SEC (0 until next attempt)
```

The table below describes significant fields shown in this output.

Table 51: show call-router status Field Descriptions

Field	Description
Border Element ID Tag	Identifier for the border element.
Border Element State	Indicates if the border element is running.
Border Element Local IP	Local IP address of the border element.
Advertise Policy	Type of descriptors that the border element advertises to its neighbors. Default is **static**. Other values are **dynamic** and **all**.
Hopcount Value	Maximum number of border element hops through which an address resolution request can be forwarded. Default is 7.
Descriptor TTL	Time-to-live value, or the amount of time, in seconds, for which a route from a neighbor is considered valid. Range is from 1 to 2147483647. Default is 1800 (30 minutes).
Access Policy	Requires that a neighbor be explicitly configured for requests to be accepted.
Local Neighbor ID	Domain name reported in service relationships.
Service Relationship Status	Service relationship between two border elements is active.
Inbound Service Relationship	Inbound time-to-Live (TTL) value in number of seconds. Range is from 1 to 4294967295.
Outbound Service Relationship	Specifies the amount of time, in seconds, to establish the outbound relationship. Range is from 1 to 65535.
Retry interval	Retry value between delivery attempts, in number of seconds. Range is from 1 to 3600.

Related Commands

Command	Description
advertise	Controls the type of descriptors that the border element advertises to its neighbors.
call -router	Enables the Annex G border element configuration commands.

Command	Description
hopcount	Specifies the maximum number of border element hops through which an address resolution request can be forwarded.
local	Defines the local domain, including the IP address and port border elements that the border element should use for interacting with remote border elements.
shutdown	Shuts down the Annex G border element.
ttl	Sets the expiration timer for advertisements.

show ccm-manager

To display a list of Cisco CallManager servers and their current status and availability, use the **show ccm-manager** command in privileged EXEC mode.

show ccm-manager [**backhaul** | **config-download** | **fallback-mgcp** | **hosts** | **music-on-hold** | **redundancy** | **download-tones** [**c1** | **c2**]]

Syntax Description

backhaul	(Optional) Displays information about the backhaul link.
config-download	(Optional) Displays information about the status of Media Gateway Control Protocol (MGCP) and Skinny Client Control Protocol (SCCP) configuration download.
fallback-mgcp	(Optional) Displays the status of the MGCP gateway fallback feature.
hosts	(Optional) Displays a list of each configured Cisco CallManager server in the network, together with its operational status and host IP address.
music-on-hold	(Optional) Displays information about all the multicast music-on-hold (MOH) sessions in the gateway at any given point in time.
redundancy	(Optional) Displays failover mode and status information for hosts, including the redundant link port, failover interval, keepalive interval, MGCP traffic time, switchover time, and switchback mode.
download-tones c1 | **c2**	(Optional) Displays custom tones downloaded to the gateway. The custom tone value of c1 or c2 specifies which tone information to display.

Command Default

If none of the optional keywords is specified, information related to all keywords is displayed.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.1(3)T	This command was introduced on the Cisco CallManager Version 3.0 and Cisco VG200.
12.2(2)XA	This command was implemented on the Cisco 2600 series and Cisco 3600 series.
12.2(2)XN	This command was modified to provide enhanced MGCP voice gateway interoperability to Cisco CallManager Version 3.1 for the Cisco 2600 series, Cisco 3600 series, and Cisco VG200.
12.2(11)T	This command was integrated into Cisco IOS Release 12.2(11) and the Cisco CallManager Version 3.2. It was implemented on the Cisco IAD2420 series.
12.2(15)ZJ	The download-tones [c1 | c2] keywords were added for the following platforms: Cisco 2610XM, Cisco 2611XM, Cisco 2620XM, Cisco 2621XM, Cisco 2650XM, Cisco 2651XM, Cisco 2691, Cisco 3640A, Cisco 3660, Cisco 3725, and Cisco 3745.
12.3(4)T	The keywords were integrated into Cisco IOS Release 12.3(4)T.

Release	Modification
12.3(14)T	New output was added relating to SCCP autoconfiguration.
12.4(15)XY	The display output was modified to include the number of TFTP download failures allowed.

Usage Guidelines

Use the **show ccm-manager config-download** command to determine the status of Cisco Unified Communications Manager servers and the automatic download information and statistics.

Examples

The following sample output shows the configured amplitudes, frequencies, and cadences of custom tone 1, Hong Kong:

```
Router# show ccm-manager download-tones c1
!
Custom Tone 1 : Hong Kong
Pulse dial:normal, Percent make:35%, DTMF low Amp.= 65424, high Amp.= 65446, Pcm:u-Law
                                      FXS  FXO  E&M  FXS  FXO  E&M
Dual Tone DR NF FOF FOS AOF AOF AOF AOS AOS AOS ONTF OFTF ONTS OFTS ONTT OFTT ONT4 OFT4
(optional) FOF2 FOS2 FOF3 FOS3 FOF4 FOS4 FOT FO4 AOT AO4 RCT1 RCT2 RCT3 RCT4
BUSY 0  2 480 620 -120 -120 -120 -120 -120 -120 500 500 0 0 0 0 0 0
RING_BACK           0  2   440   520 -120 -120 -120 -120 -120 -120   400   200   400  3000

CONGESTION          0  2   480   620 -200 -200 -200 -240 -240 -240   250   250     0     0

NUMBER_UNOBTAINABLE 0  2   480   620 -120 -120 -120 -120 -120 -120 65535     0     0     0

DIAL_TONE           0  2   350   440 -150 -150 -150 -150 -150 -150 65535     0     0     0

DIAL_TONE2          0  2   350   440 -150 -150 -150 -150 -150 -150 65535     0     0     0

OUT_OF_SERVICE      0  1   950     0 -150 -150 -150    0    0    0   330   330     0     0

ADDR_ACK            0  1   600     0 -240 -240 -240    0    0    0   125   125   125 65535

DISCONNECT          0  1   600     0 -150 -150 -150    0    0    0   330   330   330 65535

OFF_HOOK_NOTICE     0  2  1400  2040 -240 -240 -240 -240 -240 -240   100   100     0     0

OFF_HOOK_ALERT      0  2  1400  2040 -240 -240 -240 -240 -240 -240   100   100     0     0

WAITING             0  0     0     0    0    0    0    0    0    0     0     0     0     0

CONFIRM             0  0     0     0    0    0    0    0    0    0     0     0     0     0

CNFWRN_J            0  1   950     0 -170 -170 -190    0    0    0   100   100   100 65535

CNFWRN_D            0  1   600     0 -170 -170 -190    0    0    0   100   100   100 65535

STUTT_DIALTONE      0  2   350   440 -150 -150 -150 -150 -150 -150   100   100   100   100
   100   100 65535     0
PERM_SIG_TONE       0  1   480     0 -170 -170 -170    0    0    0 65535     0     0     0
WAITING1            0  0     0     0    0    0    0    0    0    0     0     0     0     0

WAITING2            0  0     0     0    0    0    0    0    0    0     0     0     0     0

WAITING3            0  0     0     0    0    0    0    0    0    0     0     0     0     0

WAITING4            0  0     0     0    0    0    0    0    0    0     0     0     0     0

MSGWAIT_IND         0  0     0     0    0    0    0    0    0    0     0     0     0     0
```

```
OFF_HOOK_WARN        0  0     0     0    0    0    0    0    0    0     0     0     0     0

Sequence Tone        DR NF F1C1  F2C1   AOF   AOS  C1ONT C1OFT C2ONT C2OFT C3ONT C3OFT C4ONT
 C4OFT  F1C2  F2C2  F1C3  F2C3  F1C4  F2C4
INTERCEPT            0  0     0     0     0     0      0     0     0     0     0     0
TONE_ON_HOLD         0  0     0     0     0     0      0     0     0     0     0     0
NO_CIRCUIT           0  0     0     0     0     0      0     0     0     0     0     0
Legend:
DR: direction NF: number of frequency FO<F,S,T,4>: frequency of<1st,2nd,3rd,4th>  AO<F,S,T,4>:
 amplitude of<1st,2nd,3rd,4th>
FOF<1-4>: frequency of 1st, cadence<1-4> FOS<1-4>: frequency of 2nd, cadence<1-4>
RCT<1-4>: repeat count for cadence<1-4>  F(1-4>C<1-4> : frequency<1-4> of cadence<1-4>
C<1-4>ONT: cadence<1-4> on time C<1-4>OFT: cadence<1-4> off time
```

The three tables below and give descriptions of significant fields once the tones are automatically downloaded to the gateway.

Table 52: show ccm-manager download-tones Significant Output Fields

Field	Description
Percent make	Pulse ratio in percentage of make.
DTMF low Amp.	Low frequency level.
high Amp.	High frequency level.
Pcm	Pulse Code Modulation (mu-law or a-law).

Table 53: show ccm-manager download-tones Output Fields for Dual Tones

Field of Dual Tone	Description
DR	Direction to PSTN (0) or Packet Network (1).
NF	Number of Frequency (from 1 to 4).
FOF	Frequency of First component (in Hz).
FXS AOF	Amplitude of First component (from 1 to 65535 = +3 dBm0) for the foreign exchange station (FXS).
FXO AOF	Amplitude of First component (from 1 to 65535 = +3 dBm0) for the foreign exchange office (FXO).
E&M AOF	Amplitude of First component (from 1 to 65535 = +3 dBm0) for the recEive and transMit (E&M).
FXS AOS	Amplitude of Second component (from 1 to 65535 = +3 dBm0) for the FXS.
FXO AOS	Amplitude of Second component (from 1 to 65535 = +3 dBm0) for the FXO.
E&M AOS	Amplitude of Second component (from 1 to 65535 = +3 dBm0) for the E&M.
ONTF	On time; time the tone is generated (milliseconds) for the first frequency.
OFTF	Off time; silence time (milliseconds) for the first frequency.

Field of Dual Tone	Description
ONTS	On time; time the tone is generated (milliseconds) for the second frequency.
OFTS	Off time; silence time (milliseconds) for the second frequency.
ONTT	On time; time the tone is generated (milliseconds) for the third frequency.
OFTT	Off time; silence time (milliseconds) for the third frequency.
ONT4	On time; time the tone is generated (milliseconds) for the fourth frequency.
OFT4	Off time; silence time (milliseconds) for the fourth frequency.
FOF2	Frequency of First component for the second cadence.
FOS2	Frequency of Second component for the second cadence.
FOF3	Frequency of First component for the third cadence.
FOS3	Frequency of Second component for the third cadence.
FOF4	Frequency of First component for the fourth cadence.
FOS4	Frequency of Second component for the fourth cadence.
FOT	Frequency of Third component (in Hertz).
FO4	Frequency of Fourth component (in Hertz).
AOT	Amplitude of Third component (from 1 to 65535 = +3 dBm0).
AO4	Amplitude of Fourth component (from 1 to 65535 = +3 dBm0).
RCT1	Number of repeat for the first cadence.
RCT2	Number of repeat for the second cadence.
RCT3	Number of repeat for the third cadence.
RCT4	Number of repeat for the fourth cadence.

Table 54: show ccm-manager download-tones Output Fields for Sequence Tones

Field of Sequence Tone	Description
DR	Direction to PSTN (0) or Packet Network (1).
NF	Number of Frequency (from 1 to 4).
F1C1	Frequency 1 of Cadence 1.
F2C1	Frequency 2 of Cadence 1.
AOF	Amplitude of First component (from 1 to 65535).

Field of Sequence Tone	Description
AOS	Amplitude of Second component (from 1 to 65535).
C1ONT	Cadence 1 On Time.
C1OFT	Cadence 1 Off Time.
C2ONT	Cadence 2 On Time.
C2OFT	Cadence 2 Off Time.
C3ONT	Cadence 3 On Time.
C3OFT	Cadence 3 Off Time.
C4ONT	Cadence 4 On Time.
C4OFT	Cadence 4 Off Time.
F1C2	Frequency 1 of Cadence 2.
F2C2	Frequency 2 of Cadence 2.
F1C3	Frequency 1 of Cadence 3.
F2C3	Frequency 2 of Cadence 3.
F1C4	Frequency 1 of Cadence 4.
F2C4	Frequency 2 of Cadence 4.

The following is sample output from the **show ccm-manager** command for displaying the status and availability of both the primary and the backup Cisco Unified Communications Manager server:

```
Router# show ccm-manager
MGCP Domain Name: Router2821.cisco.com
Priority        Status                  Host
============================================================
Primary         Registered              10.78.236.222
First Backup    None
Second Backup   None
Current active Call Manager:    10.78.236.222
Backhaul/Redundant link port:   2428
Failover Interval:              30 seconds
Keepalive Interval:             15 seconds
Last keepalive sent:            21:48:37 UTC Nov 4 2007 (elapsed time: 00:00:15)
Last MGCP traffic time:         21:48:51 UTC Nov 4 2007 (elapsed time: 00:00:02)
Last failover time:             None
Last switchback time:           None
Switchback mode:                Graceful
MGCP Fallback mode:             Not Selected
Last MGCP Fallback start time:  None
Last MGCP Fallback end time:    None
MGCP Download Tones:            Disabled
TFTP retry count to shut Ports: 3
PRI Backhaul Link info:
    Link Protocol:      TCP
    Remote Port Number: 2428
```

```
    Remote IP Address:  172.20.71.38
    Current Link State: OPEN
    Statistics:
        Packets recvd:   1
        Recv failures:   0
        Packets xmitted: 3
        Xmit failures:   0
    PRI Ports being backhauled:
       Slot 1, port 1
MGCP Download Tones:             Enabled
Configuration Auto-Download Information
=======================================
Current version-id: {1645327B-F59A-4417-8E01-7312C61216AE}
Last config-downloaded:00:00:49
Current state: Waiting for commands
Configuration Download statistics:
        Download Attempted             : 6
          Download Successful          : 6
          Download Failed              : 0
        Configuration Attempted        : 1
          Configuration Successful     : 1
          Configuration Failed(Parsing): 0
          Configuration Failed(config) : 0
Last config download command: New Registration
Configuration Error History:
FAX mode: cisco
```

The table below describes the significant fields shown in the display.

Table 55: show ccm-manager Field Descriptions

Field	Description
MGCP Domain Name (system)	System used in the Internet for translating domain names of network nodes into IP addresses.
Priority	Priority of the Cisco CallManager servers present in the network. Possible priorities are primary, first backup, and second backup.
Status	Current usage of the Cisco Unified Communications Manager server. Values are Registered, Idle, Backup Polling, and Undefined.
Host	Host IP address of the Cisco CallManager server.
Current active Call Manager	IP address of the active Cisco Communications Manager server. This field can be the IP address of any one of the following Cisco Communications Manager servers: Primary, First Backup, and Second Backup.
Backhaul/Redundant link port	Port that the Cisco CallManager server is to use.
Failover Interval	Maximum amount of time that can elapse without the gateway receiving messages from the currently active Cisco Call Manager before the gateway switches to the backup Cisco Call Manager.
Keepalive Interval	Interval following which, if the gateway has not received any messages from the currently active Cisco Communications Manager server within the specified amount of time, the gateway sends a keepalive message to the Cisco Communications Manager server to determine if it is operational.

Field	Description
Last keepalive sent	Time in hours (military format), minutes and seconds at which the last keepalive message was sent.
Last MGCP traffic time	Time in hours (military format), minutes and seconds at which the last MGCP traffic message was sent.
Switchback mode	Displays the switchback mode configuration that determines when the primary Cisco CallManager server is used if it becomes available again while a backup Cisco CallManager server is being used. Values that can appear in this field are Graceful, Immediate, *Schedule -time, and* Uptime-delay.
MGCP Fallback mode	Displays the MGCP fallback mode configuration. If "Not Selected" displays, then fallback is not configured. If "Enabled/OFF" displays, then fallback is configured but not in effect. If "Enabled/ON" displays, then fallback is configured and in effect.
Last MGCP Fallback start time	Start time stamp in hours (military format), minutes and seconds of the last fallback.
Lasts MGCP Fallback end time	End time stamp in hours (military format), minutes and seconds of the last fallback.
MGCP Download Tones	Displays if the customized tone download is enabled.
TFTP retry count to shut Ports	Number of TFTP download failures allowed before endpoints are shutdown.

The following is sample output from the **show ccm-manager config-download**command showing the status of the SCCP download:

```
Router# show ccm-manager config-download
Configuration Auto-Download Information
=======================================
Current version-id:{4171F93A-D8FC-49D8-B1C4-CE33FA8095BF}
Last config-downloaded:00:00:47
Current state:Waiting for commands
Configuration Download statistics:
        Download Attempted             :6
          Download Successful          :6
          Download Failed              :0
        Configuration Attempted        :1
          Configuration Successful     :1
          Configuration Failed(Parsing):0
          Configuration Failed(config) :0
Last config download command:New Registration
SCCP auto-configuration status
================================================================
Registered with Call Manager: No
Local interface: FastEthernet0/0 (000c.8522.6910)
Current version-id: {D3A886A2-9BC9-41F8-9DB2-0E565CF51E5A}
Current config applied at: 04:44:45 EST Jan 9 2003
Gateway downloads succeeded: 1
Gateway download attempts: 1
Last gateway download attempt:  04:44:45 EST Jan 9 2003
Last successful gateway download: 04:44:45 EST Jan 9 2003
```

```
Current TFTP server: 10.2.6.101
Gateway resets: 0
Gateway restarts: 0
Managed endpoints: 6
Endpoint downloads succeeded: 6
Endpoint download attempts: 6
Last endpoint download attempt:  04:44:45 EST Jan 9 2003
Last successful endpoint download: 04:44:45 EST Jan 9 2003
Endpoint resets: 0
Endpoint restarts: 0
Configuration Error History:
sccp ccm CCM-PUB7 identifier 1
end
controller T1 2/0no shut
controller T1 2/0no shut
controller T1 2/0no shut
isdn switch-type primary-ni
end
```

The table below describes the significant fields shown in the display.

Table 56: show ccm-manager config-download Field Descriptions

Field	Description
Current state	Current configuration state.
Download Attempted	Number of times the gateway has tried to download the configuration file. The number of successes and failures is displayed.
Configuration Attempted	Number of times the gateway has tried to configure the gateway based on the configuration file. The number of successes and failures is displayed.
Managed endpoints	Number of SSCP-controlled endpoints (analog and BRI phones).
Endpoint downloads succeeded	Number of times the gateway has successfully downloaded the configuration files for SCCP-controlled endpoints.
Endpoint download attempts	Number of times the gateway has tried to download the configuration files for SCCP-controlled endpoints.
Endpoint resets	Number of SCCP gateway resets.
Endpoint restarts	Number of SCCP gateway restarts.
Configuration Error History	Displays SCCP autoconfiguration errors.

The following is sample output from the show ccm-manager fallback-mgcp command:

```
Router# show ccm-manager fallback-mgcp
Current active Call Manager:   172.20.71.38
MGCP Fallback mode:            Enabled/OFF
Last MGCP Fallback start time: 00:14:35
Last MGCP Fallback end time:   00:17:25
```

The table below displays te mode. Modes are as follows:

Table 57: show ccm-manager fallback-mgcp modes

Field	Description
MGCP Fallback mode	The following are displayed: • Not Selected--Fallback is not configured. • Enabled/OFF--Fallback is configured but not in effect. • Enabled/ON--Fallback is configured and in effect.
Last MGCP Fallback start time	Start time stamp in hh:mm:ss of the last fallback.
Last MGCP Fallback end time	End time stamp in hh:mm:ss of the last fallback.

The following is sample output from the show ccm-manager music-on-hold command:

```
Router# show ccm-manager music-on-hold
Current active multicast sessions :1
 Multicast       RTP port   Packets       Call   Codec    Incoming
 Address         number     in/out        id              Interface
=====================================================================
172.20.71.38     2428        5/5          99      g711
```

The table below describes the significant fields shown in the display.

Table 58: show ccm-manager music-on-hold Field Descriptions

Field	Description
Current active multicast sessions	Number of active calls on hold.
Multicast Address	Valid class D address from which the gateway is getting the RTP streams.
RTP port number	Valid RTP port number on which the gateway receives the RTP packets.
Packets in/out	Number of RTP packets received and sent to the digital signal processor (DSP).
Call id	Call ID of the call that is on hold.
Codec	Codec number.
Incoming Interface	Interface through which the gateway is receiving the RTP stream.

Related Commands

Command	Description
ccm-manager config	Supplies the local MGCP voice gateway with the IP address or logical name of the TFTP server from which to download XML configuration files and enable the download of the configuration.
debug ccm-manager	Displays debugging information about the Cisco CallManager.

Command	Description
show ccm-manager	Displays a list of Cisco CallManager servers, their current status, and their availability.
show ccm-manager fallback-mgcp	Displays the status of the MGCP gateway fallback feature.
show isdn status	Displays the Cisco IOS gateway ISDN interface status.
show mgcp	Displays the MGCP configuration information.

show cdapi

To display the Call Distributor Application Programming Interface (CDAPI), use the **show cdapi**command in privileged EXEC mode.

show cdapi

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.0(7)T	This command was introduced on the Cisco AS5300.
12.3(4)T	This command was enhanced to display V.120 call types registering with the modem.

Usage Guidelines

CDAPI is the internal application programming interface (API) that provides an interface between signaling stacks and applications.

Examples

The following is sample output from the **show cdapi** command. The output displays the following information:

- Signaling stacks that register with CDAPI
- Applications that register with CDAPI
- Active calls
- Call type of each active call
- Message buffers in use

```
Router# show cdapi
Registered CDAPI Applications/Stacks
====================================
Signaling Stack: ISDN
        Interface: Se6/0:23
Application: TSP CDAPI Application Voice
        Application Type(s) : Voice Data Facility Signaling V110 V120
        Application Level   : Tunnel
        Application Mode    : Enbloc
Application: TSP CDAPI Application COT
        Application Type(s) : Cot
        Application Level   : Tunnel
        Application Mode    : Enbloc
Application: CSM
        Application Type(s) : Modem V110 V120
        Application Level   : Basic
        Application Mode    : Enbloc
Signaling Stack: XCSP
Application: dialer
        Application Type(s) : Data
```

```
        Application Level   : Basic
        Application Mode    : Enbloc
Active CDAPI Calls
==================
        Se7/7:23 Call ID = 0x7717, Call Type = V.120, Application = CSM
CDAPI Message Buffers
=====================
Free Msg Buffers: 320
Free Raw Buffers: 320
Free Large-Raw Buffers: 120
```

Field descriptions should be self-explanatory. However, the following information may be of help:

- Enbloc is the mode where all call-establishment information is sent in the setup message (opposite of overlap mode, where additional messages are needed to establish the call).
- Cot is the Continuity Test (COT) subsystem that supports the continuity test required by the Signaling System 7 (SS7) network to conduct loopback and tone check testing on the path before a circuit is established.

Related Commands

Command	Description
debug cdapi	Displays information about the CDAPI.

show ces clock-select

To display the setting of the network clock for the specified port, use the **show ces clock-select**command in privileged EXEC mode.

show ces *slot/port clock-select*

Syntax Description

slot	Backplane slot number.
/port	Interface port number. The slash must be entered.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.1(2)T	This command was introduced on the Cisco 3600 series.

Examples

The following is sample output from this command for slot 1, port 0:

```
Router# show ces 1/0 clock-select
Priority 1 clock source:not configured
Priority 2 clock source:not configured
Priority 3 clock source:ATM1/0 UP
Priority 4 clock source:Local oscillator
Current clock source:ATM1/0, priority:3
```

Field descriptions should be self-explanatory.

Related Commands

Command	Description
clock-select	Establishes the sources and priorities of the requisite clocking signals for the OC-3/STM-1 ATM Circuit Emulation Service network module.

show connect

To display configuration information about drop-and-insert connections that have been configured on a router, use the **show connect**command in privileged EXEC mode.

show connect {**all** | **elements** | **name** | **id** | **port** {**T1** | **E1**}*slot/port*}

Syntax Description

all	Information for all configured connections.
elements	Information for registered hardware or software interworking elements.
name	Information for a connection that has been named by using the **connect** global configuration command. The name you enter is case sensitive and must match the configured name exactly.
id	Information for a connection that you specify by an identification number or range of identification numbers. The router assigns these IDs automatically in the order in which they were created, beginning with 1. The **show connect all**command displays these IDs.
port	Information for a connection that you specify by indicating the type of controller (T1 or E1) and location of the interface.
T1	T1 controller.
E1	E1 controller.
slot/port	Location of the T1 or E1 controller port whose connection status you want to see. Valid values for *slot* and *port* are **0**and **1**. The slash must be entered.

Command Default

No default behavior or values

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.0(5)XK	This command was introduced on the Cisco 2600 series and Cisco 3600 series.
12.0(7)T	This command was integrated into Cisco IOS Release 12.0(7)T.

Usage Guidelines

This command shows drop-and-insert connections on modular access routers that support drop-and-insert. It displays different information in different formats, depending on the keyword that you use.

Examples

The following examples show how the same tabular information appears when you enter different keywords:

```
Router# show connect all
ID   Name               Segment 1            Segment 2           State
============================================================================
1    Test              -T1 1/0 01           -T1 1/1 02           ADMIN UP
2    Test2             -T1 1/0 03           -T1 1/1 04           ADMIN UP
```

```
Router# show connect id 1-2
ID   Name               Segment 1            Segment 2           State
=========================================================================
1    Test              -T1 1/0 01           -T1 1/1 02           ADMIN UP
2    Test2             -T1 1/0 03           -T1 1/1 04           ADMIN UP
Router# show connect port t1 1/1
ID   Name               Segment 1            Segment 2           State
=========================================================================
1    Test              -T1 1/0 01           -T1 1/1 02           ADMIN UP
2    Test2             -T1 1/0 03           -T1 1/1 04           ADMIN UP
```

The following examples show details about specific connections, including the number of time slots in use and the switching elements:

```
Router# show connect id 2
Connection: 2 - Test2
 Current State: ADMIN UP
 Segment 1: -T1 1/0 03
  TDM timeslots in use: 14-18 (5 total)
 Segment 2: -T1 1/1 04
  TDM timeslots in use: 14-18
Internal Switching Elements: VIC TDM Switch
Router# show connect name Test
 Connection: 1 - Test
 Current State: ADMIN UP
 Segment 1: -T1 1/0 01
  TDM timeslots in use: 1-13 (13 total)
 Segment 2: -T1 1/1 02
  TDM timeslots in use: 1-13
Internal Switching Elements: VIC TDM Switch
```

Field descriptions should be self-explanatory.

Related Commands

Command	Description
connect	Defines connections between T1 or E1 controller ports for Drop and Insert.
tdm-group	Configures a list of time slots for creating clear channel groups (pass-through) for TDM cross-connect.

show controllers rs366

To display information about the RS-366 video interface on the video dialing module (VDM), use the **show controllers rs366**command in privileged EXEC mode.

show controllers rs366 *slot port*

Syntax Description

slot	Slot location of the VDM module. Valid entries are 1 or 2.
port	Port location of the EIA/TIA-366 interface in the VDM module.

Command Default

No default behavior or values

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.0(5)XK	This command was introduced on the Cisco MC3810.
12.0(7)T	This command was integrated into Cisco IOS Release 12.0(7)T.

Examples

The following example displays information about the RS-366 controller:

```
Router# show controllers rs366 0 1
RS366:driver is initialized in slot 1, port 0:
STATUS STATE LSR  LCR  ICSR EXT  T1     T2     T3     T4     T5
0x02   0x01  0x00 0x50 0xE0 0x00 5000   5000   5000   20000  10000
Dial string:
121C
```

The table below describes significant fields shown in this output.

Table 59: show controllers rs366 Field Descriptions

Field	Description
STATUS	Last interrupt status.
STATE	Current state of the state machine.
LSR	Line status register of the VDM.
LCR	Line control register of the VDM.
ICSR	Interrupt control and status register of the VDM.
EXT	Extended register of the VDM.
T1 through T5	Timeouts 1 through 5 of the watchdog timer, in milliseconds.

Field	Description
Dial string	Most recently dialed number collected by the driver. 0xC at the end of the string indicates the EON (end of number) character.

show controllers timeslots

To display the channel-associated signaling (CAS) and ISDN PRI state in detail, use the show controllers timeslots command in privileged EXEC mode.

show controllers t1/e1 *controller-number* **timeslots***timeslot-range*

Syntax Description

tl/e1 *controller -number*	Controller number of CAS or ISDN PRI time slot. Range is from 0 to 7.
timeslots *timeslot -range*	Timeslot. E1 range is from 1 to 31. T1 range is from 1 to 24.

Command Default

No default behavior or values

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
10.0	This command was introduced.
12.1(3)T	The **timeslots** keyword was added.
12.1(5)T	This command was implemented on the Cisco AS5400.

Usage Guidelines

Use this command to display the CAS and ISDN PRI channel state in detail. The command shows whether the DS0 channels of a controller are in idle, in-service, maintenance, or busyout states. Use the **show controllers e1** or **show controllers t1** command to display statistics about the E1 or T1 links.

Examples

The following example shows that the CAS state is enabled on the Cisco AS5300 with a T1 PRI card:

```
Router# show controllers timeslots
T1 1 is up:
Loopback: NONE
DS0  Type       Modem    <->     Service       Channel       Rx          Tx
                                 State         State        A B C D     A B C D
-------------------------------------------------------------------------------
  1    cas-modem   1       in     insvc       connected    1  1  1  1    1  1  1  1
  2    cas         -       -      insvc       idle         0  0  0  0    0  0  0  0
  3    cas         -       -      insvc       idle         0  0  0  0    0  0  0  0
  4    cas         -       -      insvc       idle         0  0  0  0    0  0  0  0
  5    cas         -       -      insvc       idle         0  0  0  0    0  0  0  0
  6    cas         -       -      insvc       idle         0  0  0  0    0  0  0  0
  7    cas         -       -      insvc       idle         0  0  0  0    0  0  0  0
  8    cas         -       -      insvc       idle         0  0  0  0    0  0  0  0
  9    cas         -       -      insvc       idle         0  0  0  0    0  0  0  0
  10   cas         -       -      maint      static-bo     0  0  0  0    1  1  1  1
  11   cas         -       -      maint      static-bo     0  0  0  0    1  1  1  1
  12   cas         -       -      maint      static-bo     0  0  0  0    1  1  1  1
  13   cas         -       -      maint      static-bo     0  0  0  0    1  1  1  1
  14   cas         -       -      maint      static-bo     0  0  0  0    1  1  1  1
  15   cas         -       -      maint      static-bo     0  0  0  0    1  1  1  1
```

```
 16   cas         -       -      maint      static-bo     0  0  0  0    1  1  1  1
 17   cas         -       -      maint      static-bo     0  0  0  0    1  1  1  1
 18   cas         -       -      maint      static-bo     0  0  0  0    1  1  1  1
 19   cas         -       -      maint      dynamic-bo    0  0  0  0    1  1  1  1
 20   cas         -       -      maint      dynamic-bo    0  0  0  0    1  1  1  1
 21   cas         -       -      maint      dynamic-bo    0  0  0  0    1  1  1  1
 22   unused
 23   unused
 24   unused
```

The following example shows that the ISDN PRI state is enabled on the Cisco AS5300 with a T1 PRI card:

```
T1 2 is up:
Loopback: NONE
DS0 Type         Modem    <->  Service   Channel     Rx        Tx
                               State     State       A B C D   A B C D
-------------------------------------------------------------------------------
 1  pri          -        -    insvc     idle
 2  pri          -        -    insvc     idle
 3  pri          -        -    insvc     idle
 4  pri          -        -    insvc     idle
 5  pri          -        -    insvc     idle
 6  pri          -        -    insvc     idle
 7  pri          -        -    insvc     idle
 8  pri          -        -    insvc     idle
 9  pri          -        -    insvc     idle
10  pri          -        -    insvc     idle
11  pri          -        -    insvc     idle
12  pri          -        -    insvc     idle
13  pri          -        -    insvc     idle
14  pri          -        -    insvc     idle
15  pri          -        -    insvc     idle
16  pri          -        -    insvc     idle
17  pri          -        -    insvc     idle
18  pri          -        -    insvc     idle
19  pri          -        -    insvc     idle
20  pri          -        -    insvc     idle
21  pri-modem    2        in   insvc     busy
22  pri-modem    1        out  insvc     busy
23  pri-digi     -        in   insvc     busy
24  pri-sig      -        -    outofsvc  reserved
```

Field descriptions should be self-explanatory.

Related Commands

Command	Description
show controllers e1	Displays information about E1 links.
show controllers t1	Displays information about T1 links.

show controllers voice

To display information about voice-related hardware, use the **show controllers voice** command inprivileged EXEC mode.

show controllers voice

Syntax Description

This command has no arguments or keywords.

Command Default

No default behavior or values

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.0(5)XQ	This command was introduced on the Cisco 1750.

Usage Guidelines

This command displays interface status information that is specific to voice-related hardware, such as the registers of the TDM switch, the host port interface of the digital signal processor (DSP), and the DSP firmware versions. The information displayed is generally useful only for diagnostic tasks performed by technical support.

Examples

The following is sample output from this command:

```
Router# show controllers voice
EPIC Switch registers:
STDA 0xFF STDB 0xFF SARA 0xAD SARB 0xFF SAXA 0xFF SAXB 0x0 STCR 0x3F
MFAIR 0x3F
STAR 0x65 OMDR 0xE2 VNSR 0x0 PMOD 0x4C PBNR 0xFF POFD 0xF0 POFU 0x18
PCSR 0x1 PICM 0x0 CMD1 0xA0 CMD2 0x70 CBNR 0xFF CTAR 0x2 CBSR 0x20 CSCR
0x0
DSP 0 Host Port Interface:
HPI Control Register 0x202
InterfaceStatus 0x2A MaxMessageSize 0x80
RxRingBufferSize 0x6 TxRingBufferSize 0x9
pInsertRx 0x4 pRemoveRx 0x4 pInsertTx 0x6 pRemoveTx 0x6
Rx Message 0:
packet_length 100 channel_id 2 packet_id 0 process id 0x1
0000:   0000 4AC7 5F08 91D1 0000 0000 7DF1 69E5 63E1 63E2
0020:   6E7C ED67 DE5D DB5C DC60 EC7E 6BE1 58D3 50CD 4DCE
0040:   50D2 5AE5 7868 DA52 CE4A C746 C647 C94B D25A EAF4
0060:   5DD7 4FCD 4ACA 4ACC 4FD3 5DE8 F769 DC58 D352 D253
0080:   D65B E573 6CDF 59D3 4ECF 4FD0
Rx Message 1:
packet_length 100 channel_id 1 packet_id 0 process id 0x1
0000:   0000 1CDD 3E48 3B74 0000 0000 3437 3D4C F0C8 BBB5
0020:   B2B3 B7BF D25B 4138 3331 3339 435F CFBD B6B2 B1B4
0040:   BBC8 7E48 3B34 3131 363D 4FDE C3B9 B3B1 B3B8 C2DB
0060:   533F 3833 3235 3B48 71CC BDB7 B4B5 B8BF CF67 483D
0080:   3836 383C 455B DAC6 BDB9 B9BB
Rx Message 2:
packet_length 100 channel_id 2 packet_id 0 process id 0x1
0000:   0000 4AC8 5F08 9221 0000 0000 54DA 61F5 EF60 DA53
```

```
0020:   CF4F CD4E D256 DB63 FCEE 5FDA 55D1 50CF 4FD3 56D8
0040:   5DE1 6E7C EC60 DC59 D655 D456 D85D DF6A F4F4 69E2
0060:   5CDD 5BDC 5BDE 61E9 6DF1 FF76 F16D E96A E566 EA6A
0080:   EB6F F16D EF79 F776 F5F5 73F0
Rx Message 3:
packet_length 100 channel_id 1 packet_id 0 process id 0x1
0000:   0000 1CDE 3E48 3BC4 0000 0000 C0CC EC54 453E 3C3C
0020:   3F47 56F3 D1C7 C1BF C0C6 CEE1 6752 4A46 4648 4E59
0040:   6FE4 D6CF CDCE D2DA E57E 675E 5B5B 5E62 6B76 FCF6
0060:   F6FA 7D75 7373 7BF5 EAE1 DCDA DADD E6FE 6559 514D
0080:   4D4E 5563 EFD9 CDC8 C5C6 CAD1
Rx Message 4:
packet_length 100 channel_id 2 packet_id 0 process id 0x1
0000:   0000 4AC6 5F08 9181 0000 0000 DD5B DC5E E161 E468
0020:   FAFD 6CE1 5AD3 53D1 53D7 61EC EA59 CF4A C644 C344
0040:   CA4E D86C 60D0 48C2 3EBD 3CBD 3EC0 47CF 5976 DF4F
0060:   C945 C242 C146 C94E D668 73DB 54CE 4DCC 4DCE 53DB
0080:   64F9 ED63 DC59 DA58 DC5D E46C
Rx Message 5:
packet_length 100 channel_id 1 packet_id 0 process id 0x1
0000:   0000 1CDC 3E48 3B24 0000 0000 5B5B 5D62 6A76 FCF5
0020:   F5F9 7D78 7374 7CF5 EAE1 DDDA DBDD E7FE 6559 514E
0040:   4D4F 5663 EFD8 CDC8 C6C6 CAD1 E760 4E46 403F 4047
0060:   5173 D5C7 BFBC BCBE C5D4 6D4C 3F3B 3939 3D46 5ADB
0080:   C5BC B7B6 B8BD C8E8 4F3F 3835
Tx Message 0:
packet_length 100 channel_id 1 packet_id 0 process id 0x1
0000:   0000 4AC6 5F08 9181 0000 003C DD5B DC5E E161 E468
0020:   FAFD 6CE1 5AD3 53D1 53D7 61EC EA59 CF4A C644 C344
0040:   CA4E D86C 60D0 48C2 3EBD 3CBD 3EC0 47CF 5976 DF4F
0060:   C945 C242 C146 C94E D668 73DB 54CE 4DCC 4DCE 53DB
0080:   64F9 ED63 DC59 DA58 DC5D E46C
Tx Message 1:
packet_length 100 channel_id 2 packet_id 0 process id 0x1
0000:   0000 1CDC 3E48 3B24 0000 003C 5B5B 5D62 6A76 FCF5
0020:   F5F9 7D78 7374 7CF5 EAE1 DDDA DBDD E7FE 6559 514E
0040:   4D4F 5663 EFD8 CDC8 C6C6 CAD1 E760 4E46 403F 4047
0060:   5173 D5C7 BFBC BCBE C5D4 6D4C 3F3B 3939 3D46 5ADB
0080:   C5BC B7B6 B8BD C8E8 4F3F 3835
Tx Message 2:
packet_length 100 channel_id 1 packet_id 0 process id 0x1
0000:   0000 4AC7 5F08 91D1 0000 003C 7DF1 69E5 63E1 63E2
0020:   6E7C ED67 DE5D DB5C DC60 EC7E 6BE1 58D3 50CD 4DCE
0040:   50D2 5AE5 7868 DA52 CE4A C746 C647 C94B D25A EAF4
0060:   5DD7 4FCD 4ACA 4ACC 4FD3 5DE8 F769 DC58 D352 D253
0080:   D65B E573 6CDF 59D3 4ECF 4FD0
Tx Message 3:
packet_length 100 channel_id 2 packet_id 0 process id 0x1
0000:   0000 1CDD 3E48 3B74 0000 003C 3437 3D4C F0C8 BBB5
0020:   B2B3 B7BF D25B 4138 3331 3339 435F CFBD B6B2 B1B4
0040:   BBC8 7E48 3B34 3131 363D 4FDE C3B9 B3B1 B3B8 C2DB
0060:   533F 3833 3235 3B48 71CC BDB7 B4B5 B8BF CF67 483D
0080:   3836 383C 455B DAC6 BDB9 B9BB
Tx Message 4:
packet_length 100 channel_id 1 packet_id 0 process id 0x1
0000:   0000 4AC8 5F08 9221 0000 003C 54DA 61F5 EF60 DA53
0020:   CF4F CD4E D256 DB63 FCEE 5FDA 55D1 50CF 4FD3 56D8
0040:   5DE1 6E7C EC60 DC59 D655 D456 D85D DF6A F4F4 69E2
0060:   5CDD 5BDC 5BDE 61E9 6DF1 FF76 F16D E96A E566 EA6A
0080:   EB6F F16D EF79 F776 F5F5 73F0
Tx Message 5:
packet_length 100 channel_id 2 packet_id 0 process id 0x1
0000:   0000 1CDE 3E48 3BC4 0000 003C C0CC EC54 453E 3C3C
0020:   3F47 56F3 D1C7 C1BF C0C6 CEE1 6752 4A46 4648 4E59
```

```
0040:   6FE4 D6CF CDCE D2DA E57E 675E 5B5B 5E62 6B76 FCF6
0060:   F6FA 7D75 7373 7BF5 EAE1 DCDA DADD E6FE 6559 514D
0080:   4D4E 5563 EFD9 CDC8 C5C6 CAD1
Tx Message 6:
packet_length 100 channel_id 2 packet_id 0 process id 0x1
0000:   0000 1CDA 3E48 3A84 0000 003C E75F 4E46 403F 4147
0020:   5174 D5C7 BFBC BCBE C5D4 6C4C 3F3B 3939 3D46 5BDA
0040:   C5BC B7B6 B8BD C8E9 4F3F 3834 3437 3D4C EEC8 BBB5
0060:   B2B3 B8BF D35A 4138 3331 3339 435F CEBD B6B1 B1B4
0080:   BBC9 7C48 3B34 3131 363D 4FDE
Tx Message 7:
packet_length 100 channel_id 1 packet_id 0 process id 0x1
0000:   0000 4AC5 5F08 9131 0000 003C 66DE 66EB 67EE FE6E
0020:   F7E7 6B68 E068 EE6A DF5C DF62 EDF1 6FF2 7A78 67DC
0040:   5EDF 62E7 64E6 66E0 7071 EA69 F86E E260 DE5D E665
0060:   EB75 F0FB 6DE9 64E4 69E3 66EA 67E9 6DF9 F177 EC6E
0080:   EB6E F876 F875 7D6E E966 E05D
Tx Message 8:
packet_length 100 channel_id 2 packet_id 0 process id 0x1
0000:   0000 1CDB 3E48 3AD4 0000 003C C2B9 B3B1 B3B8 C2DC
0020:   523F 3733 3235 3C49 72CB BDB7 B4B5 B8BF CF67 483C
0040:   3836 373C 455C DAC6 BDB9 B9BB C0CC EE54 453E 3C3C
0060:   3F47 56F1 D1C7 C1BF C0C6 CEE1 6651 4A46 4648 4D59
0080:   70E3 D6CF CDCE D2D9 E67E 675E
Bootloader 1.8, Appn 3.1
Application firmware 3.1.8, Built by claux on Thu Jun 17 11:00:05 1999
VIC Interface Foreign Exchange Station 0/0, DSP instance (0x19543C0)
Singalling channel num 128 Signalling proxy 0x0 Signaling dsp 0x19543C0
tx outstanding 0, max tx outstanding 32
ptr 0x0, length 0x0, max length 0x0
dsp_number 0, Channel ID 1
received 0 packets, 0 bytes, 0 gaint packets
0 drops, 0 no buffers, 0 input errors 0 input overruns
650070 bytes output, 4976 frames output, 0 output errors, 0 output
underrun
0 unaligned frames
VIC Interface Foreign Exchange Station 0/1, DSP instance (0x1954604)
Singalling channel num 129 Signalling proxy 0x0 Signaling dsp 0x1954604
tx outstanding 0, max tx outstanding 32
ptr 0x0, length 0x0, max length 0x0
dsp_number 0, Channel ID 2
received 0 packets, 0 bytes, 0 gaint packets
0 drops, 0 no buffers, 0 input errors 0 input overruns
393976 bytes output, 3982 frames output, 0 output errors, 0 output
underrun
0 unaligned frames
```

Field descriptions are hardware-dependent and are meant for use by trained technical support.

Related Commands

Command	Description
show dial-peer voice	Displays configuration information and call statistics for dial peers.
show interface dspfarm	Displays hardware information including DRAM, SRAM, and the revision-level information on the line card.
show voice dsp	Displays the current status of all DSP voice channels.
show voice port	Displays configuration information about a specific voice port.

show crm

To display the carrier call capacities statistics, use the **show crm** command in privileged EXEC mode.

show crm

Syntax Description

This command has no arguments or keywords.

Command Default

No default behavior or values

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.2(11)T	This command was introduced.

Usage Guidelines

Both the **show trunk group**commandand the **show crm** command display values for the maximum number of calls. These values originate from different configuration procedures:

- In the **show trunk group** command, the Max Calls value originates from the **max-calls** command in the trunk group configuration.
- In the **show crm** command, Max calls indicates the maximum number of available channels after the carrier ID or trunk group label is assigned to an interface using the **trunk-group** (interface) command.

Examples

The following example illustrates the carrier call capacities statistics:

```
Router# show crm
Carrier:1411
    Max calls:4
    Max Voice (in) :      4    Cur Voice (in) :      0
    Max Voice (out):      4    Cur Voice (out):      0
    Max Data (in)  :      4    Cur Data (in)  :      0
    Max Data (out) :      4    Cur Data (out) :      0
Trunk Group Label: 100
    Max calls:6
    Max Voice (in) :      6    Cur Voice (in) :      0
    Max Voice (out):      6    Cur Voice (out):      0
    Max Data (in)  :      6    Cur Data (in)  :      0
    Max Data (out) :      6    Cur Data (out) :      0
```

The table below describes the fields shown in this output, in alphabetical order.

Table 60: show crm Field Descriptions

Field	Description
Carrier	ID of the carrier that handles the calls.
Cur Data (in)	Current number of incoming data calls that are handled by the carrier or trunk group.

Field	Description
Cur Data (out)	Current number of outgoing data calls that are handled by the carrier or trunk group.
Cur Voice (in)	Current number of incoming voice calls that are handled by the carrier or trunk group.
Cur Voice (out)	Current number of outgoing voice calls that are handled by the carrier or trunk group.
Max Calls	Maximum number of calls that are handled by the carrier or trunk group.
Max Data (in)	Maximum number of incoming data calls that are handled by the carrier or trunk group.
Max Data (out)	Maximum number of outgoing data calls that are handled by the carrier or trunk group.
Max Voice (in)	Maximum number of incoming voice calls that are handled by the carrier or trunk group.
Max Voice (out)	Maximum number of outgoing voice calls that are handled by the carrier or trunk group.
Trunk Group Label	Label of the trunk group that handles the calls.

Related Commands

Command	Description
carrier-id (dial-peer)	Specifies the carrier associated with VoIP calls.
max-calls	Specifies the maximum number of calls handled by a trunk group.
show trunk group	Displays the configuration parameters for one or more trunk groups.
trunk-group (interface)	Assigns an interface to a trunk group.
trunk-group-label (dial-peer)	Specifies the trunk group associated with VoIP calls.

show csm

To display the call switching module (CSM) statistics for a particular digital signal processor (DSP) channel, all DSP channels, or a specific modem or DSP channel, use the **show csm**command in privileged EXEC mode.

Cisco AS5300 Universal Access Server
show csm {**call-rate** [**table**] | **callre-source** | **modem** [*slot/port* | **group** *modem-group-number*] | **signaling-channel**}

Cisco AS5400Series Router
show csm {**call rate** [**table**] | **call-resource** | **modem** [*slotport* | **group** *modem-group-number*] | **signaling-channel** | **voice** *slot/port*}

Syntax Description

call-rate	Displays the incoming and outgoing call switching rate.
table	(Optional) Displays the incoming and outgoing call switching rate in the form of numerical table.
call-resource	Displays statistics about the CSM call resource.
modem	Displays CSM call statistics for modems.
slot / *port*	(Optional) Location (and thereby identity) of a specific modem.
group	(Optional) Displays modem group information.
modem -group-number	(Optional) Location of a particular dial peer. Range: 1 to 32767.
signaling-channel	Displays CSM signaling channel Information.
voice	Displays CSM call statistics for DSP channels.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
11.3 NA	This command was introduced.
12.0(3)T	This command was modified. Port-specific values for the Cisco AS5300 were added.
12.0(7)T	This command was modified. Port-specific values for the Cisco AS5800 were added.

Usage Guidelines

This command shows the information related to CSM, which includes the DSP channel, the start time of the call, the end time of the call, and the channel on the controller used by the call.

Use the **show csm modem** command to display the CSM call statistics for a specific modem, for a group of modems, or for all modems. If a *slot* / *port* argument is specified, then CSM call statistics are displayed for the specified modem. If the *modem-group-number*argument is specified, the CSM call statistics for all of the

modems associated with that modem group are displayed. If no keyword is specified, CSM call statistics for all modems on the Cisco AS5300 universal access server are displayed.

Use the **show csm voice** command to display CSM statistics for a particular DSP channel. If the *slot* / *dspm* / *dsp* / *dsp-channel* or *shelf* / *slot* / *port*argumentis specified, the CSM call statistics for calls using the identified DSP channel are displayed. If no argument is specified, all CSM call statistics for all DSP channels are displayed.

Examples

The following is sample output from the **show csm** command for the Cisco AS5300 universal access server:

```
Router# show csm voice 2/4/4/0
 slot 2, dspm 4, dsp 4, dsp channel 0,
 slot 2, port 56, tone, device_status(0x0002): VDEV_STATUS_ACTIVE_CALL.
csm_state(0x0406)=CSM_OC6_CONNECTED, csm_event_proc=0x600E2678, current call thru PRI line
invalid_event_count=0, wdt_timeout_count=0
wdt_timestamp_started is not activated
wait_for_dialing:False, wait_for_bchan:False
pri_chnl=TDM_PRI_STREAM(s0, u0, c22), tdm_chnl=TDM_DSP_STREAM(s2, c27)
dchan_idb_start_index=0, dchan_idb_index=0, call_id=0xA003, bchan_num=22
csm_event=CSM_EVENT_ISDN_CONNECTED, cause=0x0000
ring_no_answer=0, ic_failure=0, ic_complete=0
dial_failure=0, oc_failure=0, oc_complete=3
oc_busy=0, oc_no_dial_tone=0, oc_dial_timeout=0
remote_link_disc=0, stat_busyout=0
oobp_failure=0
call_duration_started=00:06:53, call_duration_ended=00:00:00, total_call_duration=00:00:44
The calling party phone number = 408
The called party phone number  = 5271086
total_free_rbs_timeslot = 0, total_busy_rbs_timeslot = 0, total_dynamic_busy_rbs_timeslot
= 0, total_static_busy_rbs_timeslot = 0,
total_sw56_rbs_timeslot = 0, total_sw56_rbs_static_bo_ts = 0,
total_free_isdn_channels = 21, total_busy_isdn_channels = 0,total_auto_busy_isdn_channels
= 0,
min_free_device_threshold = 0
```

The table below describes the significant fields shown in the display.

Table 61: show csm voice Field Descriptions

Field	Description
slot	Slot where the VFC resides.
dsp	DSP through which this call is established.
slot/port	Logical port number for the device. This is equivalent to the DSP channel number. The port number is derived as follows: • (max_number_of_dsp_channels per dspm=12) * the dspm # (0-based) + • (max_number_of_dsp_channels per dsp=2) * the dsp # (0-based) + the dsp channel number (0-based).

Field	Description
tone	Which signaling tone is being used (DTMF, MF, R2). This only applies to CAS calls. Possible values are as follows: • mf • dtmf • r2-compelled • r2-semi-compelled • r2-non-compelled
device_status	Status of the device. Possible values are as follows: • VDEV_STATUS_UNLOCKED--Device is unlocked (meaning that it is available for new calls). • VDEV_STATUS_ACTIVE_WDT--Device is allocated for a call and the watchdog timer is set to time the connection response from the central office. • VDEV_STATUS_ACTIVE_CALL--Device is engaged in an active, connected call. • VDEV_STATUS_BUSYOUT_REQ--Device is requested to busyout; does not apply to voice devices. • VDEV_STATUS_BAD--Device is marked as bad and not usable for processing calls. • VDEV_STATUS_BACK2BACK_TEST--Modem is performing back-to-back testing (for modem calls only). • VDEV_STATUS_RESET--Modem needs to be reset (for modem only). • VDEV_STATUS_DOWNLOAD_FILE--Modem is downloading a file (for modem only). • VDEV_STATUS_DOWNLOAD_FAIL--Modem has failed during downloading a file (for modem only). • VDEV_STATUS_SHUTDOWN--Modem is not powered up (for modem only). • VDEV_STATUS_BUSY--Modem is busy (for modem only). • VDEV_STATUS_DOWNLOAD_REQ--Modem is requesting connection (for modem only).

Field	Description
csm_state	

Field	Description
	CSM call state of the current call (PRI line) associated with this device. Possible values are as follows: • CSM_IDLE_STATE--Device is idle. • CSM_IC_STATE--A device has been assigned to an incoming call. • CSM_IC1_COLLECT_ADDR_INFO--A device has been selected to perform ANI/DNIS address collection for this call. ANI/DNIS address information collection is in progress. The ANI/DNIS is used to decide whether the call should be processed by a modem or a voice DSP. • CSM_IC2_RINGING--The device assigned to this incoming call has been told to get ready for the call. • CSM_IC3_WAIT_FOR_SWITCH_OVER--A new device is selected to take over this incoming call from the device collecting the ANI/DNIS address information. • CSM_IC4_WAIT_FOR_CARRIER--This call is waiting for the CONNECT message from the carrier. • CSM_IC5_CONNECTED--This incoming call is connected to the central office. • CSM_IC6_DISCONNECTING--This incoming call is waiting for a DISCONNECT message from the VTSP module to complete the disconnect process. • CSM_OC_STATE --An outgoing call is initiated. • CSM_OC1_REQUEST_DIGIT--The device is requesting the first digit for the dial-out number. • CSM_OC2_COLLECT_1ST_DIGIT--The first digit for the dial-out number has been collected. • CSM_OC3_COLLECT_ALL_DIGIT--All the digits for the dial-out number have been collected. • CSM_OC4_DIALING--This call is waiting for a dsx0 (B channel) to be available for dialing out. • CSM_OC5_WAIT_FOR_CARRIER--This (outgoing) call is waiting for the central office to connect. • CSM_OC6_CONNECTED--This (outgoing) call is connected. • CSM_OC7_BUSY_ERROR--A busy tone has been sent to the device (for VoIP call, no busy tone is sent; just a DISCONNECT INDICATION message is sent to the VTSP module), and this call is waiting for a DISCONNECT message from the VTSP module (or ONHOOK message from the modem) to complete the disconnect process. • CSM_OC8_DISCONNECTING--The central office has disconnected this (outgoing) call, and the call is waiting for a DISCONNECT message

Field	Description
	from the VTSP module to complete the disconnect process.
csm_state: invalid_event_count	Number of invalid events received by the CSM state machine.
wdt_timeout_count	Number of times the watchdog timer is activated for this call.
wdt_timestamp_started	Whether the watchdog timer is activated for this call.
wait_for_dialing	Whether this (outgoing) call is waiting for a free digit collector to become available to dial out the outgoing digits.
wait_for_bchan	Whether this (outgoing) call is waiting for a B channel to send the call out on.
pri_chnl	Which type of TDM stream is used for the PRI connection. For PRI and CAS calls, it is always TDM_PRI_STREAM.
tdm_chnl	Which type of TDM stream is used for the connection to the device used to process this call. In the case of a VoIP call, this is always set to TDM_DSP_STREAM.
dchan_idb_start_index	First index to use when searching for the next IDB of a free D channel.
dchan_idb_index	Index of the currently available IDB of a free D channel.
csm_event	Event just passed to the CSM state machine.
cause	Event cause.
ring_no_answer	Number of times a call failed because there was no response.
ic_failure	Number of failed incoming calls.
ic_complete	Number of successful incoming calls.
dial_failure	Number of times a connection failed because there was no dial tone.
oc_failure	Number of failed outgoing calls.
oc_complete	Number of successful outgoing calls.
oc_busy	Number of outgoing calls whose connection failed because there was a busy signal.
oc_no_dial_tone	Number of outgoing calls whose connection failed because there was no dial tone.
oc_dial_timeout	Number of outgoing calls whose connection failed because the timeout value was exceeded.
call_duration_started	Start of this call.

Field	Description
call_duration_ended	End of this call.
total_call_duration	Duration of this call.
The calling party phone number	Calling party number as given to CSM by ISDN.
The called party phone number	Called party number as given to CSM by ISDN.
total_free_rbs_time slot	Total number of free RBS (CAS) time slots available for the whole system.
total_busy_rbs_time slot	Total number of RBS (CAS) time slots that have been busied-out. This includes both dynamically and statically busied out RBS time slots.
total_dynamic_busy_rbs_time slot	Total number of RBS (CAS) time slots that have been dynamically busied out.
total_static_busy_rbs_time slot	Total number of RBS (CAS) time slots that have been statically busied out (that is, they are busied out using the CLI command).
total_free_isdn_channels	Total number of free ISDN channels.
total_busy_isdn_channels	Total number of busy ISDN channels.
total_auto_busy_isdn_channels	Total number of ISDN channels that are automatically busied out.

Related Commands

Command	Description
show call active voice	Displays the contents of the active call table.
show call history voice	Displays the contents of the call history table.
show num-exp	Displays how number expansions are configured.
show voice port	Displays configuration information about a specific voice port.

show csm call

To view the call switching module (CSM) call statistics, use the **show csm call** command in privileged EXEC mode

show csm call {**failed** | **rate** | **total**}

Syntax Description

failed	CSM call fail/reject rate for the last 60 seconds, 60 minutes, and 72 hours.
rate	CSM call rate for the last 60 seconds, 60 minutes, and 72 hours.
total	Total number of CSM calls for the last 60 seconds, 60 minutes, and 72 hours.

Command Default

No default behavior or values.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.3(2)T	This command was introduced on the Cisco AS5850.

Usage Guidelines

Use this command to understand CSM call volume.

Examples

The following examples show the CSM call statistics for the last 60 seconds:

```
Router# show csm call rate

  15
  14
  13
  12
  11
  10
   9
   8
   7
   6
   5
   4
   3
   2
   1
    0....5....1....1....2....2....3....3....4....4....5....5....
              0    5    0    5    0    5    0    5    0    5
          CSM call switching rate per second (last 60 seconds)
          # = calls entering the module per second

Router# show csm call failed
```

```
 15
 14
 13
 12
 11
 10
  9
  8
  7
  6
  5
  4
  3
  2
  1
   0....5....1....1....2....2....3....3....4....4....5....5....
             0    5    0    5    0    5    0    5    0    5
        CSM call fail/reject rate per second (last 60 seconds)
          # = calls failing per second


Router# sh csm call total


1344
1244
1144
1044
 944
 844
 744
 644
 544
 444
 344
 244
 144
  44
    0....5....1....1....2....2....3....3....4....4....5....5....
              0    5    0    5    0    5    0    5    0    5
                  CSM total calls (last 60 seconds)
```

 # = number of calls

Field descriptions should be self-explanatory.

show cube debug category codes

To display Cisco Unified Border Element debug category code information, use the **show cube debug category codes** command in user EXEC or privileged EXEC mode.

show cube debug category codes

Syntax Description

This command has no arguments or keywords.

Command Modes

User EXEC (>)

Privileged EXEC (#)

Command History

Release	Modification
15.3(3)M	This command was introduced.

Example

```
Device# show cube debug category codes
|-----------------------------------------------
| show cube debug category codes values.
|-----------------------------------------------
| Indx |  Debug Name           |   Value
|-----------------------------------------------
|  01  |  SDP Debugs           |   1
|  02  |  Audio Debugs         |   2
|  03  |  Video Debugs         |   4
|  04  |  Fax Debugs           |   8
|  05  |  SRTP Debugs          |   16
|  06  |  DTMF Debugs          |   32
|  07  |  SIP Profiles Debugs  |   64
|  08  |  SDP Passthrough Deb  |   128
|  09  |  Transcoder Debugs    |   256
|  10  |  SIP Transport Debugs |   512
|  11  |  Parse Debugs         |   1024
|  12  |  Config Debugs        |   2048
|  13  |  Control Debugs       |   4096
|  14  |  Miscellaneous Debugs |   8192
|  15  |  Supp Service Debugs  |   16384
|  16  |  Misc  Features Debugs|   32768
|  17  |  SIP Line-side Debugs |   65536
|  18  |  CAC Debugs           |   131072
|  19  |  Registration Debugs  |   262144
|-----------------------------------------------
```

show cube status

To display the Cisco Unified Border Element (CUBE) status, the software version, the license capacity, the image version, and the platform name of the device, use the **show cube status** command in user EXEC or privileged EXEC mode.

show cube status

Syntax Description

This command has no arguments or keywords.

Command Default

In releases before Cisco IOS XE Amsterdam 17.2.1r, CUBE status is not displayed unless license capacity is configured using mode border-element command.

Effective from Cisco IOS XE Amsterdam 17.2.1r, the dependency on configuring license capacity is removed.

Command Modes

User EXEC (>)

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Amsterdam 17.3.2 and Cisco IOS XE Bengaluru 17.4.1a	This command was modified to support Cisco Smart Licensing Using Policy.
Cisco IOS XE Amsterdam 17.2.1r	The dependency on **mode border-element license capacity** *sessions* command was removed. Licensed-Capacity and blocked call information was excluded from output.
15.1(3)S1	This command was modified. The output was modified to have only token characters (an alphanumeric character, hyphen [-], dot [.], exclamation mark [!], percent [%], asterisk [*], underscore [_], plus sign [+], grave [`], apostrophe ['], or a tilde [~]) in server and user-agent Session Initiation Protocol (SIP) headers. The nontoken characters present in the image name is replaced by a dot[.].
15.2(1)T	This command was introduced.

Usage Guidelines

In releases before Cisco IOS XE Amsterdam 17.2.1r, the CUBE status display is enabled only if the **mode border-element** command is configured with call license capacity. The **show cube status** command displays the following message if the license capacity is not configured

```
Cisco Unified Border Element (CUBE) application is not enabled
```

Effective from Cisco IOS XE Amsterdam 17.2.1r, CUBE status display is enabled without configuring **mode border-element license capacity** *sessions* command. Licensed-Capacity and blocked call information is excluded from output.

CUBE status information is also available using Simple Network Management Protocol (SNMP) with the CISCO-UBE-MIB MIB.

Examples

Example - Releases before Cisco IOS XE Amsterdam 17.2.1r

The following example configures the **mode border-element** command with call license capacity and enables the display of CUBE status on the Cisco 3845 router:

```
Device(config)# voice service voip
Device(conf-voi-serv)# mode border-element license capacity 200
```

After saving the configuration and reloading the device:

```
Device> show cube status

CUBE-Version : 11.0.0
SW-Version : 15.5(2)T, Platform 3845
HA-Type : none
Licensed-Capacity : 200
```

In Cisco IOS Release 15.1(3)S1 and later releases, the output is as follows:

```
Device> show cube status

CUBE-Version : 8.8
SW-Version : 15.2.1.T, Platform 3845
HA-Type : none
Licensed-Capacity : 200
```

Example - Release Cisco IOS XE Amsterdam 17.2.1r and later

From Cisco IOS XE Amsterdam 17.2.1r onwards, the output is displayed as follows:

```
Device> show cube status

CUBE-Version : 12.7.0
SW-Version : 16.12.20191014.105214, Platform CSR1000V
HA-Type : hot-standby-chassis-to-chassis
```

Examples

The table below describes the fields shown in the display.

Table 62: show cube status Field Descriptions

Field	Description
CUBE-Version	Version of the CUBE application running on the device.
SW-Version	Image version and platform name of the device running the CUBE application. This matches the image version and platform name returned by the **show version** command.
HA-Type	The type of High Availability (HA) feature configured and running on the device. The following HA types are supported: • none: CUBE does not support HA. • cold-standby-chassis-to-chassis: Device-to-device cold standby support. • hot-standby-chassis-to-chassis: Device-to-device hot standby support.

Field	Description
Licensed-Capacity	**Note** Effective from Cisco IOS XE Amsterdam 17.2.1r, Licensed-Capacity and blocked call information is no longer included in the output. Number of SIP call legs that CUBE is licensed to use. The range is from 0 through 999999. This number matches the number of licenses configured using the **mode border-element license capacity** command. **Note** The number of SIP call legs that CUBE can use is platform-dependent and is not affected by the specified value for the **capacity** keyword in Cisco IOS Release 15.2(1)T.

Related Commands

Command	Description
mode border-element	Enables the set of commands used in the border-element configuration on the Cisco 2900 and Cisco 3900 series platforms.

show debug condition

To display the debugging filters that have been enabled for VoiceXML applications, ATM-enabled interfaces, or Frame Relay interfaces, use the **show debug condition** command in privileged EXEC mode.

show debug condition

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.2(11)T	This command was introduced on the Cisco 3640, Cisco 3660, Cisco AS5300, Cisco AS5350, and Cisco AS5400.
12.0(28)S	This command was integrated into Cisco IOS Release 12.0(28)S and was enhanced to include debugging for ATM-enabled and Frame Relay-enabled interfaces.
12.2(25)S	This command was integrated into Cisco IOS Release 12.2(25)S.
12.2(27)SBC	This command was integrated into Cisco IOS Release 12.2(27)SBC.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.4(9)T	This command was enhanced to include debugging for ATM-enabled and Frame Relay-enabled interfaces.

Usage Guidelines

This command displays the debugging filter conditions that have been set for VoiceXML applications by using the **debug condition application voice** command.

Examples

The following is sample output from this command when it is used with the VoiceXML application:

```
Router# show debug condition
Condition 1: application voice vmail (1 flags triggered)
       Flags: vmail
Condition 2: application voice myapp1 (1 flags triggered)
       Flags: myapp1
```

The following is sample output from this command when an ATM interface is being debugged:

```
Router# show debug condition

Condition 1: atm-vc 0/56784 AT2/0 (0 flags triggered)
Condition 2: atm-vc 255/45546 AT2/0 (0 flags triggered)
Condition 3: atm-vc 0/266 AT6/0 (1 flags triggered)
```

The table below describes the significant fields shown in the display.

Table 63: show debug condition Field Descriptions

Field	Description
Condition 1	Sequential number identifying the filter condition that was set for the specified command.
Flags	Name of the voice application for which the condition was set.
at2/0	Interface number of the ATM interface that has the debug condition applied.
atm-vc 0/56784	Virtual channel identifier (VCI). Alternatively, virtual path identifier/virtual channel identifier (VCI/VPI) pair.

Related Commands

Command	Description
debug condition application voice	Filters out debugging messages for all VoiceXML applications except the specified application.
debug http client	Displays debugging messages for the HTTP client.
debug vxml	Displays debugging messages for VoiceXML features.



show dial-peer through show gatekeeper zone prefix

- show dial-peer, on page 396
- show dial-peer video, on page 397
- show dial-peer voip keepalive status, on page 398
- show dial-peer voice, on page 400
- show dialplan dialpeer, on page 411
- show dialplan incall, on page 417
- show dialplan incall uri, on page 420
- show dialplan in-carrier, on page 426
- show dialplan in-trunk-group-label, on page 428
- show dialplan number, on page 430
- show dialplan uri, on page 433
- show dn-numbers, on page 435
- show dspfarm, on page 437
- show dspfarm profile, on page 445
- show dsp-group, on page 448
- show echo-cancel, on page 450
- show event-manager consumers, on page 452
- show frame-relay vofr, on page 454
- show gatekeeper calls, on page 456
- show gatekeeper circuits, on page 458
- show gatekeeper cluster, on page 460
- show gatekeeper endpoint circuits, on page 461
- show gatekeeper endpoints, on page 463
- show gatekeeper gw-type-prefix, on page 466
- show gatekeeper performance statistics, on page 468
- show gatekeeper servers, on page 472
- show gatekeeper status, on page 474
- show gatekeeper status cluster, on page 476
- show gatekeeper zone cluster, on page 477
- show gatekeeper zone prefix, on page 478
- show gatekeeper zone status, on page 480

show dial-peer

To display the dial plan mapping table for protocol peers, use the **show dial-peer**command in privileged EXEC mode.

show dial-peer {**carrier** | **cor** | **trunk-group-label**}

Syntax Description

carrier	Displays carrier ID configuration details of the peer protocol.
cor	Displays restriction settings class details.
trunk-group-label	Displays trunk group label configuration details.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.2(17)SX	This command was introduced.
12.4(22)T	This command was modified in a release earlier than Cisco IOS Release 12.4(22)T. The **carrier** and **trunk-group-label**keywords were added.

Usage Guidelines

Use this command to display the dial plan mapping table for protocol peers along with the available keywords.

Examples

The following sample output from the **show dial-peer** command displays restriction settings class details. The fields are self-explanatory.

```
Router# show dial-peer cor
Class of Restriction
name: class1
```

show dial-peer video

To display configuration information for video dial peers, use the **show dial-peer video**command in privileged EXEC mode.

show dial-peer video [*number*] [**summary**]

Syntax Description

number	(Optional) A specific video dial peer. Output displays information about that dial peer.
summary	(Optional) Output displays a one-line summary of each video dial peer.

Command Default

If both the *name* argument and **summary** keyword are omitted, command output displays detailed information about all video dial peers.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.0(5)XK	This command was introduced on the Cisco MC3810.
12.0(7)T	This command was integrated into Cisco IOS Release 12.0(7)T.

Usage Guidelines

Use this command to display the configuration for all video dial peers configured for a router. To show configuration information for only one specific dial peer, use the *number* argument to identify the dial peer.

Examples

The following sample output displays detailed information about all configured video dial peers:

```
Router# show dial-peer video
Video Dial-Peer 1
      type = videocodec, destination-pattern = 111
      port signal = 1/0, port media = Serial1
      nsap = 47.0091810000000050E201B101.00107B09C6F2.C8
Video Dial-Peer 2
      type = videoatm,   destination-pattern = 222
      session-target = ATM0 svc nsap 47.0091810000000050E201B101.00E01E92ADC2.C8
Video Dial-Peer 3
      type = videoatm,   destination-pattern = 333
      session-target = ATM0 pvc 70/70
```

The table below describes the significant fields shown in the output.

Table 64: show dial-peer video Field Descriptions

Field	Description
NSAP	Network service access point (NSAP) address

show dial-peer voip keepalive status

To display the status of the destination when options-keepalive is configured under dial-peer, use the **show dial-peer voip keepalive status** command in privileged EXEC mode.

show dial-peer voip keepalive status [*dp-tag* | **tenant** *tenant-tag* | **<cr>**]

dp-tag	Dial-Peer Tag. Range: 1—1073741823.
tenant-tag	Keepalive status info for tenants. Range: 1—10000.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Cupertino 17.9.1a	This command was introduced.

Usage Guidelines

Use this command to know the status of the destination when options-keepalive is configured under the dial-peer configuration mode using the command **voice-class sip options-keepalive profile**. You can use this command to display the options keepalive status for individual session targets and server groups. The keepalive status is displayed for IPv4, IPv6, and DNS format destinations.

Note CUBE does not display the status for dynamic dial-peers.

If the destination is configured as DNS SRV, the status of each of the records is maintained by CUBE. For example, if the DNS SRV lookup results in four records, the status of each of these four records is displayed. For session server groups which have multiple destinations, the keepalive status of each of these targets is displayed by the command.

The command output can be filtered also on the basis of **tenant-tag** and **dp-tag**.

The different **STATUS** for the dial-peer, as displayed by the command, include:

- **active**—The dial-peer is active and contains destinations that are available to be considered by CUBE for the routing of call handling.
- **busyout**—The dial-peer is inactive and no suitable destinations are available currently.
- **partial**—A dial-peer is marked as partially active if at least one of the destinations is active out of a group, and the rest are inactive (busyout).
- **NA**—The command **voice-class sip options-keepalive profile** is not configured and hence the status is not available.

The different **STATUS** for the different destinations, as displayed by the command, include:

- **active**—The destination is available to CUBE.
- **busyout**—The destination is marked inactive after the keepalive retries are exhausted.

Note You need to configure the same transport type for the dial-peers with same SRV destination.

Examples

The following is sample output of the command that displays the status of the dial-peer destination when options-keepalive is configured under the dial-peer:

```
router#show dial-peer voip keepalive status
 TAG         TENANT   DESTINATION                    OOD-SessID   PRI     WT      STATUS
 6           4        dns:company.com                                             partial
                       company1.com                   437          10      50      active

                       ipv4:10.105.34.88:8788
                       company2.com*                  0            10      50      busyout

 8           -        dns:ex.company.com                                          active
                       example1.com                   438          10      50      active

                       ipv4:10.105.34.88:8790
                       example2.com                   439          10      50      active

                       ipv4:10.64.86.70:8789
 9           3        ipv4:10.64.86.70:8073          1            -       -       busyout
 10          -        sess-svr-grp:1
                       ipv4:10.105.34.88:8071         2            -       -       busyout
                       ipv4:10.105.34.88:8072         3            -       -       busyout
                       ipv4:10.105.34.88:8073         4            -       -       busyout
 11          -        dns:demo3.com                                               active
                       ipv4:10.64.86.70:5060          440          -       -       active

 12          -        dns:demo_failed.com*                                        busyout
 13          -        dns:demo4.com                                               partial
                       example3.com                   441          10      50      active

                       ipv4:10.105.34.88:8792
                       example4.com*                  0            10      50      busyout

Note: For destinations that are marked with (*), DNS resolution has failed.

router#
```

Related Commands

Command	Description
show voice class sip-options-keepalive	Displays the details of connectivity between CUBE VoIP dial peers and SIP servers.

show dial-peer voice

To display information for voice dial peers, use the **show dial-peer voice** command in user EXEC or privileged EXEC mode.

show dial-peer voice [*number* | **busy-trigger-counter** | **summary** | **voip system**]

Syntax Description

number	(Optional) A specific voice dial peer. The output displays detailed information about that dial peer.
busy-trigger-counter	(Optional) Displays the busy trigger call count on the VoIP dial peer.
summary	(Optional) Displays a short summary of each voice dial peer.
voip system	(Optional) Displays information about the VoIP dial peer.

Command Default

If both the *number* argument and **summary** keyword are omitted, the output displays detailed information about all voice dial peers.

Command Modes

User EXEC (>)

Privileged EXEC (#)

Command History

Release	Modification
11.3(1)T	This command was introduced.
11.3(1)MA	This command was modified. The **summary** keyword was added for the Cisco MC3810.
12.0(3)XG	This command was implemented for Voice over Frame Relay (VoFR) on the Cisco 2600 series and Cisco 3600 series.
12.0(4)T	This command was implemented for VoFR on the Cisco 7200 series.
12.1(3)T	This command was implemented for modem pass-through over VoIP on the Cisco AS5300.
12.2(2)XB	This command was modified to support VoiceXML applications.
12.2(4)T	This command was implemented on the Cisco 1750.
12.2(8)T	This command was implemented on the Cisco 1751, Cisco 2600 series, Cisco 3600 series, Cisco 3725, and Cisco 3745.
12.2(2)XN	This command was modified. Support for enhanced Media Gateway Control Protocol (MGCP) voice gateway interoperability was added to Cisco CallManager 3.1 for the Cisco 2600 series, Cisco 3600 series, and Cisco VG200.

Release	Modification
12.2(11)T	This command was integrated into Cisco IOS Release 12.2(11)T and Cisco CallManager 3.2 and implemented on the Cisco IAD2420. The command was enhanced to display configuration information for bandwidth, video codec, and rtp payload-type for H.263+ and H.264 video codec.
12.4(22)T	This command was modified. This command was enhanced to display the current configuration state of the history-info header. Command output was updated to show IPv6 information.
15.0(1)XA	This command was modified. The output was enhanced to show the logical partitioning class of restriction (LPCOR) policy for outgoing calls.
15.1(1)T	This command was integrated into Cisco IOS Release 15.1(1)T.
15.1(3)T	This command was modified. The output was enhanced to display information about the bind at the dial-peer level and to display the connection status of Foreign Exchange Office (FXO) ports.
Cisco IOS XE Cupertino 17.9.1a	This command was modified. The output was enhanced to display the OPTIONS ping keepalive status for a dial-peer.

Usage Guidelines

Use the **show dial-peer voice** command to display the configuration for all VoIP and POTS dial peers configured for a gateway. To display configuration information for only one specific dial peer, use the *number* argument. To display summary information for all dial peers, use the **summary** keyword.



Note The recommended command to verify the QoS settings that the signaling and media packets will be marked with when RSVP is not configured for call signaling on the Cisco UBE is the **show dial-peer voice** command.

Examples

The following is sample output from the **show dial-peer voice** command for a POTS dial peer:

```
Device# show dial-peer voice 100
VoiceEncapPeer3201
peer type = voice, information type = video,
description = `',
tag = 3201, destination-pattern = `86001',
answer-address = `', preference=0,
CLID Restriction = None
CLID Network Number = `'
CLID Second Number sent
CLID Override RDNIS = disabled,
source carrier-id = `', target carrier-id = `',
source trunk-group-label = `', target trunk-group-label = `',
numbering Type = `unknown'
group = 3201, Admin state is up, Operation state is up,
Outbound state is up,
incoming called-number = `', connections/maximum = 0/unlimited,
DTMF Relay = disabled,
URI classes:
     Destination =
huntstop = disabled,
```

```
in bound application associated: 'DEFAULT'
out bound application associated: ''
dnis-map =
permission :both
        incoming COR list:maximum capability
outgoing COR list:minimum requirement
Translation profile (Incoming):
Translation profile (Outgoing):
incoming call blocking:
translation-profile = `'
disconnect-cause = `no-service'
advertise 0x40 capacity_update_timer 25 addrFamily 4 oldAddrFamily 4
type = pots, prefix = `',
forward-digits 4
session-target = `', voice-port = `2/0:23',
direct-inward-dial = enabled,
digit_strip = enabled,
register E.164 number with H323 GK and/or SIP Registrar = TRUE
fax rate = system,   payload size =  20 bytes
supported-language = ''
preemption level = `routine'
bandwidth:
     maximum = 384 KBits/sec, minimum = 64 KBits/sec
voice class called-number:
     inbound = `', outbound = `1'
Time elapsed since last clearing of voice call statistics never
        Connect Time = 0, Charged Units = 0,
Successful Calls = 0, Failed Calls = 0, Incomplete Calls = 0
Accepted Calls = 0, Refused Calls = 0,
Last Disconnect Cause is "",
Last Disconnect Text is "",
Last Setup Time = 0.
```

The following is a sample output from this command for a VoIP dial peer:

```
Device# show dial-peer voice 101
VoiceOverIpPeer101
peer type = voice, system default peer = FALSE, information type = voice,
description = `',
tag = 1234, destination-pattern = `',
voice reg type = 0, corresponding tag = 0,
allow watch = FALSE
answer-address = `', preference=0,
CLID Restriction = None
CLID Network Number = `'
CLID Second Number sent
CLID Override RDNIS = disabled,
rtp-ssrc mux = system
source carrier-id = `', target carrier-id = `',
source trunk-group-label = `',  target trunk-group-label = `',
numbering Type = `unknown'
group = 1234, Admin state is up, Operation state is down,
incoming called-number = `', connections/maximum = 0/unlimited,
DTMF Relay = disabled,
modem transport = system,
URI classes:
Incoming (Request) =
Incoming (Via) =
Incoming (To) =
Incoming (From) =
Destination =
huntstop = disabled,
```

```
in bound application associated: 'DEFAULT'
out bound application associated: ''
dnis-map =
permission :both
incoming COR list:maximum capability
outgoing COR list:minimum requirement
outgoing LPCOR:
Translation profile (Incoming):
Translation profile (Outgoing):
incoming call blocking:
translation-profile = `'
disconnect-cause = `no-service'
advertise 0x40 capacity_update_timer 25 addrFamily 4 oldAddrFamily 4
mailbox selection policy: none
type = voip, session-target = `',
technology prefix:
settle-call = disabled
ip media DSCP = ef, ip media rsvp-pass DSCP = ef
ip media rsvp-fail DSCP = ef, ip signaling DSCP = af31,
ip video rsvp-none DSCP = af41,ip video rsvp-pass DSCP = af41
ip video rsvp-fail DSCP = af41,
ip defending Priority = 0, ip preemption priority = 0
ip policy locator voice:
ip policy locator video:
UDP checksum = disabled,
session-protocol = sipv2, session-transport = system,
req-qos = best-effort, acc-qos = best-effort,
req-qos video = best-effort, acc-qos video = best-effort,
req-qos audio def bandwidth = 64, req-qos audio max bandwidth = 0,
req-qos video def bandwidth = 384, req-qos video max bandwidth = 0,
RTP dynamic payload type values: NTE = 101
Cisco: NSE=100, fax=96, fax-ack=97, dtmf=121, fax-relay=122
CAS=123, TTY=119, ClearChan=125, PCM switch over u-law=0,
A-law=8, GSMAMR-NB=117 iLBC=116, AAC-ld=114, iSAC=124
lmr_tone=0, nte_tone=0
h263+=118, h264=119
G726r16 using static payload
G726r24 using static payload
RTP comfort noise payload type = 19
fax rate = voice,   payload size =  20 bytes
fax protocol = system
fax-relay ecm enable
Fax Relay ans enabled
Fax Relay SG3-to-G3 Enabled (by system configuration)
fax NSF = 0xAD0051 (default)
codec = g729r8,   payload size =  20 bytes,
video codec = None
voice class codec = `'
voice class sip session refresh system
voice class sip rsvp-fail-policy voice post-alert mandatory keep-alive interval 30
voice class sip rsvp-fail-policy voice post-alert optional keep-alive interval 30
voice class sip rsvp-fail-policy video post-alert mandatory keep-alive interval 30
voice class sip rsvp-fail-policy video post-alert optional keep-alive interval 30
text relay = disabled
Media Setting = forking (disabled) flow-through (global)
Expect factor = 10, Icpif = 20,
Playout Mode is set to adaptive,
Initial 60 ms, Max 1000 ms
Playout-delay Minimum mode is set to default, value 40 ms
Fax nominal 300 ms
Max Redirects = 1, signaling-type = cas,
VAD = enabled, Poor QOV Trap = disabled,
Source Interface = NONE
voice class sip url = system,
```

```
voice class sip tel-config url = system,
voice class sip rel1xx = system,
voice class sip anat = system,
voice class sip outbound-proxy = "system",
voice class sip associate registered-number = system,
voice class sip asserted-id system,
voice class sip privacy system
voice class sip e911 = system,
voice class sip history-info = system,
voice class sip reset timer expires 183 = system,
voice class sip pass-thru headers = system,
voice class sip pass-thru content unsupp = system,
voice class sip pass-thru content sdp = system,
voice class sip copy-list = system,
voice class sip g729 annexb-all = system,
voice class sip early-offer forced = system,
voice class sip negotiate cisco = system,
voice class sip block 180 = system,
voice class sip block 183 = system,
voice class sip block 181 = system,
voice class sip preloaded-route = system,
voice class sip random-contact = system,
voice class sip random-request-uri validate = system,
voice class sip call-route p-called-party-id = system,
voice class sip call-route history-info = system,
voice class sip privacy-policy send-always = system,
voice class sip privacy-policy passthru = system,
voice class sip privacy-policy strip history-info = system,
voice class sip privacy-policy strip diversion = system,
voice class sip map resp-code 181 = system,
voice class sip bind control = enabled, 9.42.28.29,
voice class sip bind media = enabled, 9.42.28.29,
voice class sip bandwidth audio = system,
voice class sip bandwidth video = system,
voice class sip encap clear-channel = system,
voice class sip error-code-override options-keepalive failure = system,
voice class sip calltype-video = false
voice class sip registration passthrough = System
voice class sip authenticate redirecting-number  = system,
redirect ip2ip = disabled
local peer = false
probe disabled,
Secure RTP: system (use the global setting)
voice class perm tag = `'
Time elapsed since last clearing of voice call statistics never
Connect Time = 0, Charged Units = 0,
Successful Calls = 0, Failed Calls = 0, Incomplete Calls = 0
Accepted Calls = 0, Refused Calls = 0,
Last Disconnect Cause is "",
Last Disconnect Text is "",
Last Setup Time = 0.
Last Disconnect Time = 0.
When there is no Dial-peer level bind -
voice class sip bind control = system,
voice class sip bind media = system,
```

The following is sample output from the **show dial-peer voice summary** command that shows connected FXO port 0/2/0 (the last entry) has OUT STAT set to "up," which indicates that the POTS dial peer can be used for an outgoing call. If this port is disconnected, the status changes in the output so that the OUT STAT field reports "down," and the POTS dial peer cannot be used for an outgoing call.

Note Beginning in Cisco IOS Release 15.1(3)T, there is improved status monitoring of FXO ports--any time an FXO port is connected or disconnected, a message is displayed to indicate the status change. For example, the following message is displayed to report that a cable has been connected, and the status is changed to "up" for FXO port 0/2/0: 000118: Jul 14 18:06:05.122 EST: %LINK-3-UPDOWN: Interface Foreign Exchange Office 0/2/0, changed state to operational status up due to cable reconnection

```
Router# show dial-peer voice summary
dial-peer hunt 0
                    AD                                      PRE PASS                 OUT
TAG    TYPE  MIN  OPER PREFIX    DEST-PATTERN      FER THRU SESS-TARGET    STAT PORT
KEEPALIVE
39275- voip  up   up             .T                 0  syst ipv4:172.18.108.26
82
8880   pots  up   up             8880               0                       up   2/0/0
8881   pots  up   up             8881               0                       up   2/0/1
8882   pots  up   up             8882               0                       up   2/0/2
8883   pots  up   up             8883               0                       up   2/0/3
8884   pots  up   up             8884               0                       up   2/0/4
8885   pots  up   up             8885               0                       up   2/0/5
8886   pots  up   up             8886               0                       up   2/0/6
8887   pots  up   up             8887               0                       up   2/0/7
88888- pots  up   up                                0                     down  0/3/0:23
888
65033- pots  up   up             6503352            0                       up   0/2/0
52
```

The table below describes the significant fields shown in the displays, in alphabetical order.

Table 65: show dial-peer voice Field Descriptions

Field	Description
Accepted Calls	Number of calls accepted from this peer since system startup.
acc-qos	Lowest acceptable quality of service configured for calls for this peer.
Admin state	Administrative state of this peer.
answer-address	Answer address configured for this dial peer.
bandwidth maximum/minimum	The maximum and minimum bandwidth, in Kb/s.
Charged Units	Total number of charging units that have applied to this peer since system startup, in hundredths of a second.
CLID Restriction	Indicates if Calling Line ID (CLID) restriction is enabled.
CLID Network Number	Displays the network number sent as CLID, if configured.
CLID Second Number sent	Displays whether a second calling number is stripped from the call setup.
CLID Override RDNIS	Indicates whether the CLID is overridden by the redirecting number.

Field	Description
codec	Default voice codec rate of speech.
Connect Time	Accumulated connect time to the peer since system startup for both incoming and outgoing calls, in hundredths of a second.
connections/maximum	Indicates the maximum number of call connections per peer.
Destination	Indicates the voice class that is used to match the destination URL.
destination-pattern	Destination pattern (telephone number) for this peer.
digit_strip	Indicates if digit stripping is enabled.
direct-inward-dial	Indicates if direct inward dial is enabled.
disconnect-cause	Indicates the disconnect cause code to be used when an incoming call is blocked.
dnis-map	Name of the dialed-number identification service (DNIS) map.
DTMF Relay	Indicates if dual-tone multifrequency (DTMF) relay is enabled.
Expect factor	User-requested expectation factor of voice quality for calls through this peer.
Failed Calls	Number of failed call attempts to this peer since system startup.
fax rate	Fax transmission rate configured for this peer.
forward-digits	Indicates the destination digits to be forwarded of this peer.
group	Group number associated with this peer.
huntstop	Indicates whether dial-peer hunting is turned on, by the **huntstop** command, for this dial peer.
Icpif	Configured Impairment/Calculated Planning Impairment Factor (ICPIF) value for calls sent by a dial peer.
in bound application associated	Interactive voice response (IVR) application that is configured to handle inbound calls to this dial peer.
incall-number	Full E.164 telephone number to be used to identify the dial peer.
incoming call blocking	Indicates the incoming call blocking setup of this peer.
incoming called-number	Indicates the incoming called number if it has been set.
incoming COR list	Indicates the level of Class of Restrictions for incoming calls of this peer.
Incomplete Calls	Indicates the number of outgoing disconnected calls with the user busy (17), no user response (18), or no answer (19) cause code.

Field	Description
information type	Information type for this call (voice, fax, video).
Last Disconnect Cause	Encoded network cause associated with the last call. This value is updated whenever a call is started or cleared and depends on the interface type and session protocol being used on this interface.
Last Disconnect Text	ASCII text describing the reason for the last call termination.
Last Setup Time	Value of the system uptime when the last call to this peer was started.
Modem passthrough	Modem pass-through signaling method is named signaling event (NSE).
numbering Type	Indicates the numbering type for a peer call leg.
Operation state	Operational state of this peer.
outgoing COR list	Indicates the level of Class of Restrictions for outgoing calls of this peer.
outgoing LPCOR	Setting of the **lpcor outgoing** command.
out bound application associated	The voice application that is configured to handle outbound calls from this dial peer. Outbound calls are handed off to the named application.
Outbound state	Indicates the current outbound status of a POTS peer.
payload size	Indicates the size (in bytes) of the payload of the fax rate or codec setup.
payload type	NSE payload type.
peer type	Dial peer type (voice, data).
permission	Configured permission level for this peer.
Poor QOV Trap	Indicates if poor quality of voice trap messages is enabled.
preemption level	Indicates the call preemption level of this peer.
prefix	Indicates dialed digits prefix of this peer.
Redundancy	Packet redundancy (RFC 2198) for modem traffic.
Refused Calls	Number of calls from this peer refused since system startup.
register E.164 number with H.323 GK and/or SIP Registrar	Indicates the "register e.164" option of this peer.
req-qos	Configured requested quality of service for calls for this dial peer.
session-target	Session target of this peer.
session-protocol	Session protocol to be used for Internet calls between local and remote routers through the IP backbone.

Field	Description
source carrier-id	Indicates the source carrier ID of this peer that will be used to match the source carrier ID of an incoming call.
source trunk-group label	Indicates the source trunk group label of this peer that can be used to match the source trunk group label of an incoming call.
Successful Calls	Number of completed calls to this peer.
supported-language	Indicates the list of supported languages of this peer.
tag	Unique dial peer ID number.
target carrier-id	Indicates the target carrier ID of this peer that will be used to match the target carrier ID for an outgoing call.
target-trunkgroup-label	Indicates the target trunk group label of this peer that can be used to match the target trunk group label of an outgoing call.
Time elapsed since last clearing of voice call statistics	Elapsed time between the current time and the time when the**clear dial-peer voice** command was executed.
Translation profile (Incoming)	Indicates the translation profile for incoming calls.
Translation profile (Outgoing)	Indicates the translation profile for outgoing calls.
translation-profile	Indicates the number translation profile of this peer.
type	Indicates the peer encapsulation type (pots, voip, vofr, voatm or mmoip).
VAD	Whether voice activation detection (VAD) is enabled for this dial peer.
voice class called-number inbound/outbound	Indicates the voice-class called number inbound or outbound setup of this peer.
voice class sip history-info	Indicates the configuration state of the history-info header. If the history-info header is not configured for the dial peer, this field is set to system. If the history-info header is enabled on this dial peer, this field is set to enable. If the history-info header is disabled on this dial peer, this field is set to disable.
voice class sip bind	Indicates the configuration state of the bind address. If the bind is configured for the global, this field is sent to system. If the bind address is enabled on this dial peer, this field is set to enabled.
voice-port	Indicates the voice interface setting of this POTS peer.

The following is sample output from this command with the **summary** keyword:

```
Router# show dial-peer voice summary
dial-peer hunt 0
                                                    PASS
  TAG TYPE   ADMIN OPER PREFIX   DEST-PATTERN     PREF THRU SESS-TARGET    PORT
```

```
 100 pots    up    up                              0
 101 voip    up    up            5550112           0   syst ipv4:10.10.1.1
 102 voip    up    up            5550134           0   syst ipv4:10.10.1.1
  99 voip    up    down                            0   syst
  33 pots    up    down                            0
```

The table below describes the significant fields shown in the display.

Table 66: show dial-peer voice summary Field Descriptions

Field	Description
dial-peer hunt	Hunt group selection order that is defined for the dial peer by the **dial-peer hunt** command.
TAG	Unique identifier assigned to the dial peer when it was created.
TYPE	Type of dial peer (mmoip, pots, voatm, vofr, or voip).
ADMIN	Whether the administrative state is up or down.
OPER	Whether the operational state is up or down.
PREFIX	Prefix that is configured in the dial peer by the **prefix** command.
DEST-PATTERN	Destination pattern that is configured in the dial peer by the **destination-pattern** command.
PREF	Hunt group preference that is configured in the dial peer by the **preference** command.
PASS THRU	Modem pass-through method that is configured in the dial peer by the **modem passthrough** command.
SESS-TARGET	Destination that is configured in the dial peer by the **session target** command.
PORT	Router voice port that is configured for the dial peer. Valid only for POTS dial peers.

The following is sample output of the **show dial-peer voice summary** command that is enhanced from Cisco IOS XE Cupertino 17.9.1a to display the overall keepalive status for the DNS SRV at the dial-peer level:

```
Router# show dial-peer voice summary
dial-peer hunt 0
             AD                                      PRE PASS SESS-SER-GRP\  OUT
TAG    TYPE  MIN  OPER PREFIX    DEST-PATTERN      FER THRU SESS-TARGET    STAT PORT
KEEPALIVE    VRF
4      voip  up   up             1234               0  syst dns:example1.com
active      NA
5      voip  up   up             123456             0  syst dns:example2.com
partial     NA
44     voip  up   up             1234               0  syst dns:example3.com
busyout     NA
For server-grp details please execute command:show voice class server-group <tag_id>
To see complete session target for ipv6 use 'sh running-config | section dial-peer <tag>
Some nodes of this target may be down. Please execute the command 'show dial-peer voip
keepalive status' to know the exact status of each node.
```

Note A dial-peer is marked as partially active (**partial**) if at least one of the destinations is active out of a group, and the rest are inactive.

Related Commands

Command	Description
show call active voice	Displays the VoIP active call table.
show call history voice	Displays the VoIP call history table.
show dialplan incall number	Displays which POTS dial peer is matched for a specific calling number or voice port.
show dialplan number	Displays which dial peer is reached when a specific telephone number is dialed.
show num-exp	Displays how the number expansions are configured in VoIP.
show voice port	Displays configuration information about a specific voice port.

show dialplan dialpeer

To display the outbound dial peers that are matched to an incoming dial peer based on the class of restriction (COR) criteria and the dialed number, use the **show dialplan dialpeer** command in privileged EXEC mode.

show dialplan dialpeer incoming-dialpeer-tag number number [**timeout**]

Syntax Description

incoming-dialpeer-tag	The dial peer COR identifier used to determine the matching outbound dial peer.
number	The dialed number used in conjunction with the COR identifier to determine the matching outbound dial peer.
timeout	(Optional) Allows matching for variable-length destination patterns.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.1(3)T	This command was introduced on the Cisco 2600 series and Cisco 3600 series routers and on Cisco AS5800 access servers.
12.2(11)T	This command was implemented on the Cisco 1751 and Cisco 3700 series routers and on Cisco AS5300 access servers.

Usage Guidelines

Use this command as a troubleshooting tool to determine which outbound dial peer is matched for an incoming call, based on the COR criteria and dialed number specified in the command line. Use the timeout keyword to enable matching variable-length destination patters associated with dial peers. This can increase your chances of finding a match for the dial peer number you specify.

Note For actual voice calls coming into the router, the incoming corlist of a specified inbound dial peer and the outgoing called number will be used to match the outbound dial peer.

Examples

The following sample output shows an incoming call with a dialed number of 19001111 and meeting the COR criteria as part of dial peer 300 with incoming COR-list has been matched to an outbound dial peer with IP address 1.8.50.7:

```
Router# show dialplan dialpeer 300 number 1900111
VoiceOverIpPeer900
        information type = voice,
        description = `',
        tag = 900, destination-pattern = `1900',
        answer-address = `', preference=0,
        numbering Type = `unknown'
        group = 900, Admin state is up, Operation state is up,
        incoming called-number = `', connections/maximum = 0/unlimited,
        DTMF Relay = disabled,
        modem passthrough = system,
```

```
        huntstop = disabled,
        in bound application associated: 'DEFAULT'
        out bound application associated: ''
        dnis-map =
        permission :both
        incoming COR list:maximum capability
        outgoing COR list:to900
        type = voip, session-target = `ipv4:1.8.50.7',
        technology prefix:
        settle-call = disabled
        ...
        Time elapsed since last clearing of voice call statistics never
        Connect Time = 0, Charged Units = 0,
        Successful Calls = 0, Failed Calls = 0, Incomplete Calls = 0
        Accepted Calls = 0, Refused Calls = 0,
        Last Disconnect Cause is "",
        Last Disconnect Text is "",
        Last Setup Time = 0.
Matched: 19001111   Digits: 4
Target: ipv4:1.8.50.7
```

The table below describes the significant fields shown in the display.

Table 67: show dialplan command Field Descriptions

Field	Description
Macro Exp.	Expected destination pattern for this dial peer.
VoiceEncapPeer	Dial peer associated with the calling number entered.
VoiceOverIpPeer	Dial peer associated with the calling number entered.
peer type	Type of this dial peer (voice or data).
information type	Information type for this dial peer (voice or data).
description	Any additional information for this dial peer entered using the **description** dial peer command.
tag	Unique number identifying the dial peer.
destination-pattern	Destination pattern (telephone number) configured for this dial peer.
answer-address	Answer address (calling number) configured for this dial peer.
preference	Hunt group preference order set for this dial peer.
CLID restriction	Indicates the Caller ID restriction (if any) configured for this dial peer.
CLID Network Number	Indicates the originating network of the Caller ID source.
CLID Second Number sent	Indicates the digits in the second number (if any) forwarded for this dial peer.
source carrier-id	VoIP or POTS source carrier identifier.
source trunk-group-label	VoIP or POTS source trunk group identifier.

Field	Description
numbering Type	Identifies the numbering scheme employed for this dial peer.
group	Dial peer group in which this dial peer is a member.
Admin state	Administrative state of this dial peer.
Operation state	Operational state of this dial peer.
incoming called-number	Called number (DNIS) configured for this dial peer.
connections/maximum	Number of actual and maximum allowable connections associated with this dial peer.
DTMF Relay	Whether the **dtmf-relay** command is enabled or disabled for this dial peer.
URI classes: Incoming (Request)	URI voice class used for matching dial peer to Request-URI in an incoming SIP Invite message.
URI classes: Incoming (To)	URI voice class used for matching dial peer to the To header in an incoming SIP Invite message.
URI classes: Incoming (From)	URI voice class used for matching dial peer to the From header in an incoming SIP Invite message.
URI classes: Destination	URI voice class used to match the dial peer to the destination URI for an outgoing call.
modem transport	Transport method configured for modem calls. The default is system, which means that the value configured globally is used.
huntstop	Whether the **huntstop** command is enabled or disabled for this dial peer.
in bound application associated	IVR application that is associated with this dial peer when this dial peer is used for an inbound call leg.
out bound application associated	IVR application that is associated with this dial peer when this dial peer is used for an outbound call leg.
dnis-map	Name of the dialed-number identification service (DNIS) map that is configured in the dial peer with the **dnis-map** command.
permission	Configured permission level for this dial peer.
incoming COR list	Class of restriction (COR) criteria associated when matching an incoming dial peer.
outgoing COR list	COR criteria used to determine the appropriate outbound dial peer.
Translation profile (Incoming)	Incoming translation criteria applied to this dial peer.
Translation profile (Outgoing)	Translation criteria applied to this dial peer when matching an outbound dial peer.

Field	Description
incoming call blocking	Indicates whether or not incoming call blocking has been applied for this dial peer.
translation-profile	The predefined translation profile associated with this dial peer.
disconnect-cause	Encoded network cause associated with the last call.
voice-port	Voice port through which calls come into this dial peer.
type	Type of dial peer (POTS or VoIP).
prefix	Prefix number that is added to the front of the dial string before it is forwarded to the telephony device.
forward-digits	Which digits are forwarded to the telephony interface as configured using the **forward-digits** command.
session-target	Configured session target (IP address or host name) for this dial peer.
direct-inward-dial	Whether the **direct-inward-dial** command is enabled or disabled for this dial peer.
digit_strip	Whether digit stripping is enabled or disabled in the dial peer. Enabled is the default.
register E.164 number with GK	Indicates whether or not the dial peer has been configured to register its full E.164-format number with the local gatekeeper.
fax rate	The transmission speed configured for fax calls. The default is system, which means that the value configured globally is used.
payload size	The size (in bytes) for a fax transmission payload.
session-protocol	Session protocol to be used for Internet calls between local and remote router via the IP backbone.
req-qos	Configured requested quality of service for calls for this dial peer.
acc-qos	Lowest acceptable quality of service configured for calls for this dial peer.
codec	Voice codec configured for this dial peer. Default is G.729 (8 kbps).
Expect factor	User-requested expectation factor of voice quality for calls through this dial peer.
Icpif	Configured calculated planning impairment factor (ICPIF) value for calls sent by this dial peer.
VAD	Indicates whether or not voice activation detection (VAD) is enabled for this dial peer.

Field	Description
voice class sip url	URL format (SIP or TEL) used for SIP calls to this dial peer, as configured with the **voice-class sip url** command. The default is system, which means that the value configured globally with the **url** command in voice service VoIP SIP mode is used.
voice class sip rel1xx	Indicates whether or not reliable provisional responses are supported, as configured with the **voice-class sip rel1xx** command. The default is system, which means that the value configured globally with the **rel1xx** command in voice service VoIP SIP mode is used.
voice class perm tag	Voice class for a trunk that is assigned to this dial peer with the **voice-class permanent** command.
Connect Time	Unit of measure indicating the call connection time associated with this dial peer.
Charged Units	Number of call units charged to this dial peer.
Successful Calls	Number of completed calls to this dial peer since system startup.
Failed Calls	Number of uncompleted (failed) calls to this dial peer since system startup.
Incomplete Calls	Number of incomplete calls to this dial peer since system startup.
Accepted Calls	Number of calls from this dial peer accepted since system startup.
Refused Calls	Number of calls from this dial peer refused since system startup.
Last Disconnect Cause	Encoded network cause associated with the last call. This value is updated whenever a call is started or cleared and depends on the interface type and session protocol being used on this interface.
Last Disconnect Text	ASCII text describing the reason for the last call termination.
Last Setup Time	Value of the System Up Time when the last call to this peer was started.
Matched	Destination pattern matched for this dial peer.
Digits	Number of digits in this destination pattern matched for this dial peer.
Target	Matched session target (IP address or host name) for this dial peer.

Related Commands

Command	Description
show dialplan in-carrier	Displays which VoIP or POTS dial peer is matched for a specific source carrier.
show dialplan in-trunk-group-label	Displays which VoIP or POTS dial peer is matched for a specific source trunk group.
show dialplan incall	Displays which POTS dial peer is matched for a specific calling number or voice port.

Command	Description
show dialplan number	Displays which dial peer is matched for a particular telephone number.

show dialplan incall

To display which incoming POTS dial peer is matched for a specific calling number or voice port, use the **show dialplan incall number** command in privileged EXEC mode.

show dialplan incall *voice-port* **number** *calling-number* [**timeout**]

Syntax Description

voice -port	Voice port location. The syntax of this argument is platform-specific. For information on the syntax for a particular platform, see the **voice-port** command.
calling -number	E.164 Calling number or ANI of the incoming voice call.
timeout	(Optional) Allows matching for variable-length destination patterns.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
11.3(1)T	This command was introduced on the Cisco 3600 series.
12.2(8)T	This command was implemented on the Cisco 1751, Cisco 2600 series, Cisco 3725, and Cisco 3745 and the timeout keyword was added.

Usage Guidelines

Use this command as a troubleshooting tool to determine which POTS dial peer is matched for an incoming call, for the selected calling number and voice port. The router attempts to match these items in the order listed:

1. Calling number with answer-address configured in dial peer
2. Calling number with destination-pattern configured in dial peer
3. Voice port with voice port configured in dial peer

The router first attempts to match a dial peer based on the calling number (ANI). If the router is unable to match a dial peer based on the calling number, it matches the call to a POTS dial peer based on the selected voice interface. If more than one dial peer uses the same voice port, the router selects the first matching dial peer. Use the timeout keyword to enable matching variable-length destination patters associated with dial peers. This can increase you r chances of finding a match for the dial peer number you specify.



Note For actual voice calls coming into the router, the router attempts to match the called number (the dialed number identification service [DNIS] number) with the incoming called-number configured in a dial peer. The router, however, does not consider the called number when using the **show dialplan incall number** command.

Examples

The following sample output shows that an incoming call from interface 1/0/0:D with a calling number of 12345 is matched to POTS dial peer 10:

```
Router# show dialplan incall 1/0/0:D number 12345
Macro Exp.: 12345
VoiceEncapPeer10
        information type = voice,
        tag = 10, destination-pattern = `123..',
        answer-address = `', preference=0,
        numbering Type = `unknown'
        group = 10, Admin state is up, Operation state is up,
        incoming called-number = `', connections/maximum = 0/unlimited,
        DTMF Relay = disabled,
        huntstop = disabled,
        in bound application associated: DEFAULT
        out bound application associated:
        permission :both
        incoming COR list:maximum capability
        outgoing COR list:minimum requirement
        type = pots, prefix = `',
        forward-digits default
        session-target = `', voice-port = `1/0/0:D',
        direct-inward-dial = disabled,
        digit_strip = enabled,
        register E.164 number with GK = TRUE
        Connect Time = 0, Charged Units = 0,
        register E.164 number with GK = TRUE
        Connect Time = 0, Charged Units = 0,
        Successful Calls = 0, Failed Calls = 0,
        Accepted Calls = 0, Refused Calls = 0,
        Last Disconnect Cause is "",
        Last Disconnect Text is "",
        Last Setup Time = 0.
Matched: 12345   Digits: 3
Target:
```

The following sample output shows that, if no dial peer has a destination pattern or answer address that matches the calling number of 888, the incoming call is matched to POTS dial peer 99, because the call comes in on voice port 1/0/1:D, which is the voice port configured for this dial peer:

```
Router# show dialplan incall 1/0/1:D number 888
Macro Exp.: 888
VoiceEncapPeer99
        information type = voice,
        tag = 99, destination-pattern = `99...',
        answer-address = `', preference=1,
        numbering Type = `national'
        group = 99, Admin state is up, Operation state is up,
        incoming called-number = `', connections/maximum = 0/unlimited,
        DTMF Relay = disabled,
        huntstop = disabled,
        in bound application associated: DEFAULT
        out bound application associated:
        permission :both
        incoming COR list:maximum capability
        outgoing COR list:minimum requirement
        type = pots, prefix = `5',
        forward-digits 4
        session-target = `', voice-port = `1/0/1:D',
        direct-inward-dial = enabled,
        digit_strip = enabled,
register E.164 number with GK = TRUE
        Connect Time = 0, Charged Units = 0,
        Successful Calls = 0, Failed Calls = 0,
        Accepted Calls = 0, Refused Calls = 0,
```

```
        Last Disconnect Cause is "",
        Last Disconnect Text is "",
        Last Setup Time = 0.
Matched:    Digits: 0
Target:
```

Related Commands

Command	Description
show dialplan dialpeer	Displays which outbound dial peer is matched based upon the incoming dialed number and the COR criteria specified in the command line.
show dialplan in-carrier	Displays which VoIP or POTS dial peer is matched for a specific source carrier.
show dialplan in-trunk-group-label	Displays which VoIP or POTS dial peer is matched for a specific source trunk group.
show dialplan number	Displays which dial peer is matched for a particular telephone number.

show dialplan incall uri

To display which dial peer is matched for a specific uniform resource identifier (URI) in an incoming voice call, use the **show dialplan incall uri**command in privileged EXEC mode.

H.323 Session Protocol
show dialplan incall uri h323 {**called** | **calling**} *uri*

SIP Session Protocol
show dialplan incall uri sip {**from** | **request** | **to**} *uri*

Syntax Description

called	Voice class that is configured in dial peers with the **incoming uri called** command.
calling	Voice class that is configured in dial peers with the **incoming uri calling**command.
from	Voice class that is configured in dial peers with the **incoming uri from**command.
request	Voice class that is configured in dial peers with the **incoming uri request**command.
to	Voice class that is configured in dial peers with the **incoming uri to**command.
uri	URI of the incoming call.

Command Default

No default behavior or values

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.3(4)T	This command was introduced.

Usage Guidelines

- Use this command for troubleshooting to determine which dial peer is matched for an incoming call, based on the selected URI and the specified field in the call message.
- To set the URI format for matching calls, use the **voice class uri** command. To set the URI voice class in the inbound dial peer, use the **incoming uri** command.

Examples

The following is sample output from this command for a SIP URI:

```
Router# show dialplan incall uri sip from sip:5551234
Inbound VoIP dialpeer matching based on SIP URI's
VoiceOverIpPeer10
        peer type = voice, information type = voice,
        description = `',
        tag = 10, destination-pattern = `',
        answer-address = `', preference=0,
        CLID Restriction = None
        CLID Network Number = `'
        CLID Second Number sent
```

```
            source carrier-id = `', target carrier-id = `',
            source trunk-group-label = `',  target trunk-group-label = `',
            numbering Type = `unknown'
            group = 10, Admin state is up, Operation state is up,
            incoming called-number = `', connections/maximum = 0/unlimited,
            DTMF Relay = disabled,
            modem transport = system,
            URI classes:
                Incoming (Request) =
                Incoming (To) =
                Incoming (From) = 101
                Destination =
            huntstop = disabled,
            in bound application associated: 'get_headers_tcl'
            out bound application associated: ''
            dnis-map =
            permission :both
            incoming COR list:maximum capability
            outgoing COR list:minimum requirement
            Translation profile (Incoming):
            Translation profile (Outgoing):
            incoming call blocking:
            translation-profile = `'
            disconnect-cause = `no-service'
            type = voip, session-target = `',
            technology prefix:
            settle-call = disabled
            ip media DSCP = ef, ip signaling DSCP = af31, UDP checksum = disabled,
            session-protocol = sipv2, session-transport = system, req-qos = best-ef
            acc-qos = best-effort,
            RTP dynamic payload type values: NTE = 101
            Cisco: NSE=100, fax=96, fax-ack=97, dtmf=121, fax-relay=122
                   CAS=123, ClearChan=125, PCM switch over u-law=0,A-law=8
            RTP comfort noise payload type = 19
            fax rate = voice,   payload size =  20 bytes
            fax protocol = system
            fax-relay ecm enable
            fax NSF = 0xAD0051 (default)
            codec = g729r8,   payload size =  20 bytes,
            Expect factor = 0, Icpif = 20,
            Playout Mode is set to default,
            Initial 60 ms, Max 300 ms
            Playout-delay Minimum mode is set to default, value 40 ms
            Fax nominal 300 ms
            Max Redirects = 1, signaling-type = ext-signal,
            VAD = enabled, Poor QOV Trap = disabled,
            Source Interface = NONE
            voice class sip url = system,
            voice class sip rel1xx = system,
            voice class perm tag = `'
            Time elapsed since last clearing of voice call statistics never
            Connect Time = 0, Charged Units = 0,
            Successful Calls = 0, Failed Calls = 0, Incomplete Calls = 0
            Accepted Calls = 0, Refused Calls = 0,
            Last Disconnect Cause is "",
            Last Disconnect Text is "",
            Last Setup Time = 0.
Matched:    Digits: 0
Target:
```

The following is sample output from this command for a TEL URI:

```
Router# show dialplan incall uri h323 called tel:1234567
 Inbound VoIP dialpeer matching based on H323 URI's
```

```
VoiceOverIpPeer25
        peer type = voice, information type = voice,
        description = `',
        tag = 25, destination-pattern = `',
        answer-address = `', preference=0,
        CLID Restriction = None
        CLID Network Number = `'
        CLID Second Number sent
        source carrier-id = `', target carrier-id = `',
        source trunk-group-label = `',  target trunk-group-label = `',
        numbering Type = `unknown'
        group = 25, Admin state is up, Operation state is up,
        incoming called-number = `', connections/maximum = 0/unlimited,
        DTMF Relay = disabled,
        modem transport = system,
        URI classes:
            Incoming (Called) = 103
            Incoming (Calling) =
            Destination =
        huntstop = disabled,
        in bound application associated: 'callme'
        out bound application associated: ''
        dnis-map =
        permission :both
        incoming COR list:maximum capability
        outgoing COR list:minimum requirement
        Translation profile (Incoming):
        Translation profile (Outgoing):
        incoming call blocking:
        translation-profile = `'
        disconnect-cause = `no-service'
        type = voip, session-target = `ipv4:10.10.1.1',
        technology prefix:
        settle-call = disabled
        ip media DSCP = ef, ip signaling DSCP = af31, UDP checksum = disabled,
        session-protocol = cisco, session-transport = system, req-qos = best-ef
        acc-qos = best-effort,
        RTP dynamic payload type values: NTE = 101
        Cisco: NSE=100, fax=96, fax-ack=97, dtmf=121, fax-relay=122
               CAS=123, ClearChan=125, PCM switch over u-law=0,A-law=8
        RTP comfort noise payload type = 19
        fax rate = voice,   payload size =  20 bytes
        fax protocol = system
        fax-relay ecm enable
        fax NSF = 0xAD0051 (default)
        codec = g729r8,   payload size =  20 bytes,
        Expect factor = 0, Icpif = 20,
        Playout Mode is set to default,
        Initial 60 ms, Max 300 ms
        Playout-delay Minimum mode is set to default, value 40 ms
        Fax nominal 300 ms
        Max Redirects = 1, signaling-type = ext-signal,
        VAD = enabled, Poor QOV Trap = disabled,
        Source Interface = NONE
        voice class sip url = system,
        voice class sip rel1xx = system,
        voice class perm tag = `'
        Time elapsed since last clearing of voice call statistics never
        Connect Time = 0, Charged Units = 0,
        Successful Calls = 0, Failed Calls = 0, Incomplete Calls = 0
        Accepted Calls = 0, Refused Calls = 0,
        Last Disconnect Cause is "",
        Last Disconnect Text is "",
        Last Setup Time = 0.
```

```
Matched:    Digits: 0
Target:
```

The table below describes significant fields in the displays.

Table 68: show dialplan incall uri Field Descriptions

Field	Description
VoiceOverIpPeer	Dial peer associated with the calling number entered.
information type	Information type for this call; for example, voice or fax.
tag	Unique number that identifies the dial peer.
destination-pattern	Destination pattern (called number) configured for this dial peer.
answer-address	Answer address (calling number) configured for this dial peer.
preference	Hunt group preference order set for this dial peer.
Admin state	Administrative state of this dial peer.
Operation state	Operational state of this dial peer.
incoming called-number	Called number (DNIS) configured for this dial peer.
DTMF Relay	Whether the **dtmf-relay** command is enabled or disabled for this dial peer.
URI classes: Incoming (Request)	URI voice class used for matching dial peer to Request-URI in an incoming SIP Invite message.
URI classes: Incoming (To)	URI voice class used for matching dial peer to the To header in an incoming SIP Invite message.
URI classes: Incoming (From)	URI voice class used for matching dial peer to the From header in an incoming SIP Invite message.
URI classes: Destination	URI voice class used to match the dial peer to the destination URI for an outgoing call.
huntstop	Whether the **huntstop** command is enabled or disabled for this dial peer.
in bound application associated	IVR application that is associated with this dial peer when this dial peer is used for an inbound call leg.
out bound application associated	IVR application that is associated with this dial peer when this dial peer is used for an outbound call leg.
dnis-map	Name of the dialed-number identification service (DNIS) map that is configured in the dial peer with the **dnis-map** command.
permission	Configured permission level for this peer.
type	Type of dial peer (POTS or VoIP).

Field	Description
session-target	Configured session target (IP address or host name) for this dial peer.
session-protocol	Session protocol to be used for Internet calls between local and remote router via the IP backbone.
req-qos	Configured requested quality of service for calls for this dial peer.
acc-qos	Lowest acceptable quality of service configured for calls for this peer.
codec	Voice codec configured for this dial peer. Default is G.729 (8 kbps).
Expect factor	User-requested expectation factor of voice quality for calls through this peer.
Icpif	Configured calculated planning impairment factor (ICPIF) value for calls sent by a dial peer.
VAD	Whether voice activation detection (VAD) is enabled for this dial peer.
voice class sip url	URL format (SIP or TEL) used for SIP calls to this dial peer, as configured with the **voice-class sip url** command. The default is system, which means that the value configured globally with the **url** command in voice service VoIP SIP mode is used.
voice class sip rel1xx	Whether reliable provisional responses are supported, as configured with the **voice-class sip rel1xx** command. The default is system, which means that the value configured globally with the **rel1xx** command in voice service VoIP SIP mode is used.
voice class perm tag	Voice class for a trunk that is assigned to this dial peer with the **voice-class permanent** command.
Connect Time	Unit of measure indicating the call connection time associated with this dial peer.
Charged Units	Number of call units charged to this dial peer.
Successful Calls	Number of completed calls to this peer since system startup.
Failed Calls	Number of uncompleted (failed) calls to this peer since system startup.
Accepted Calls	Number of calls from this peer accepted since system startup.
Refused Calls	Number of calls from this peer refused since system startup.
Last Disconnect Cause	Encoded network cause associated with the last call. This value is updated whenever a call is started or cleared and depends on the interface type and session protocol being used on this interface.
Last Disconnect Text	ASCII text describing the reason for the last call termination.
Last Setup Time	Value of the System Up Time when the last call to this peer was started.

Field	Description
Matched	Destination pattern matched for this dial peer.
Target	Matched session target (IP address or host name) for this dial peer.

Related Commands

Command	Description
debug voice uri	Displays debugging messages related to URI voice classes.
incoming uri	Specifies the voice class used to match a VoIP dial peer to the URI of an incoming call.
session protocol	Specifies the session protocol in the dial peer for calls between the local and remote router.
show dial-peer voice	Displays detailed and summary information about voice dial peers.
show dialplan uri	Displays which outbound dial peer is matched for a specific destination URI.
voice class uri	Creates or modifies a voice class for matching dial peers to calls containing a SIP or TEL URI.
voice class uri sip preference	Sets a preference for selecting voice classes for a SIP URI.

show dialplan in-carrier

To display which incoming VoIP or POTS dial peer is matched for a specific source carrier or voice port, use the **show dialplan in-carrier** command in privileged EXEC mode.

show dialplan in-carrier *carrier-id* [**voip** | **pots**]

Syntax Description

carrier -id	VoIP or POTS source carrier identifier.
voip	(Optional) Allows you to limit the search criteria to only VoIP dial peers.
pots	(Optional) Allows you to limit the search criteria to only POTS dial peers.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.2(13)T	This command was introduced on the Cisco 2600 series and Cisco 3600 series routers and on Cisco AS5300, Cisco AS5400, and Cisco AS5800 access servers.

Usage Guidelines

Use this command as a troubleshooting tool to determine which VoIP or POTS dial peer is matched for an incoming call, based on the carrier identifier specified in the command line. Use the voip or pots keywords to further limit the scope of possible matches for the dial peer specified in the **show dialplan** command line.

Examples

The following sample output shows a VoIP or POTS dial peer being matched to another POTS dial peer based on its carrier identifier, "aaa":

```
Router# show dialplan in-carrier aaa pots
 Inbound pots dialpeer Matching based on source carrier-id
VoiceEncapPeer7777
        information type = voice,
        description = `',
        tag = 7777, destination-pattern = `',
        answer-address = `', preference=0,
        CLID Restriction = None
        CLID Network Number = `'
        CLID Second Number sent
        source carrier-id = `aaa',      target carrier-id = `',
        source trunk-group-label = `',  target trunk-group-label = `',
        numbering Type = `unknown'
        group = 7777, Admin state is up, Operation state is up,
        incoming called-number = `', connections/maximum = 0/unlimited,
        DTMF Relay = disabled,
        huntstop = disabled,
        in bound application associated:'DEFAULT'
        out bound application associated:''
        dnis-map =
        permission :both
        incoming COR list:maximum capability
        outgoing COR list:minimum requirement
        Translation profile (Incoming):
        Translation profile (Outgoing):
```

```
        incoming call blocking:
        translation-profile = `'
        disconnect-cause = `no-service'
voice-port = `'
        type = pots, prefix = `',
        forward-digits default
        session-target = `', up,
        direct-inward-dial = disabled,
        digit_strip = enabled,
        register E.164 number with GK = TRUE
        fax rate = system,   payload size =  20 bytes
        Time elapsed since last clearing of voice call statistics never
        Connect Time = 0, Charged Units = 0,
        Successful Calls = 0, Failed Calls = 0, Incomplete Calls = 0
        Accepted Calls = 0, Refused Calls = 0,
        Last Disconnect Cause is "",
        Last Disconnect Text is "",
        Last Setup Time = 0.
Matched:   Digits:0
Target:
```

Related Commands

Command	Description
show dialplan dialpeer	Displays which outbound dial peer is matched based upon the incoming dialed number and the COR criteria specified in the command line.
show dialplan incall	Displays which POTS dial peer is matched for a specific calling number or voice port.
show dialplan in-trunk-group-label	Displays which VoIP or POTS dial peer is matched for a specific source trunk group.
show dialplan number	Displays which dial peer is matched for a particular telephone number.

show dialplan in-trunk-group-label

To display which incoming VoIP or POTS dial peer is matched for a specific trunk group label, use the **show dialplan in-trunk-group-label** command in privileged EXEC mode.

show dialplan in-trunk-group-label *trunk-group-label* {**pots** | **voip**}

Syntax Description

trunk -group-label	VoIP or POTS source trunk group identifier.
voip	(Optional) Allows you to limit the search criteria to only VoIP dial peers.
pots	(Optional) Allows you to limit the search criteria to only POTS dial peers.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.2(13)T	This command was introduced on the Cisco 2600 series and Cisco 3600 series routers and on Cisco AS5300, Cisco AS5400, and Cisco AS5800 access servers.

Usage Guidelines

Use this command to determine which VoIP or POTS dial peer is matched for an incoming call, based on the identifier of the source trunk group. The router attempts to match these items in the order listed. Use the voip or pots keywords to further limit the scope of possible matches for the dial peer specified in the **show dialplan** command line.

Examples

The following sample output shows an inbound VoIP or POTS dial peer being matched to an outbound POTS dial peer based on the trunk group label "NYtrunk":

```
Router# show dialplan in-trunk-group-label NYtrunk pots
 Inbound pots dialpeer Matching based on source trunk-group-label
VoiceEncapPeer2003
        information type = voice,
        description = `',
        tag = 2003, destination-pattern = `',
        answer-address = `', preference=0,
        CLID Restriction = None
        CLID Network Number = `'
        CLID Second Number sent
        source carrier-id = `', target carrier-id = `',
        source trunk-group-label = `NYtrunk',   target trunk-group-label = `',
        numbering Type = `unknown'
        group = 2003, Admin state is up, Operation state is up,
        incoming called-number = `', connections/maximum = 0/unlimited,
        DTMF Relay = disabled,
        huntstop = disabled,
        in bound application associated:'debit-card'
        out bound application associated:''
        dnis-map =
        permission :both
        incoming COR list:maximum capability
        outgoing COR list:minimum requirement
        Translation profile (Incoming):
```

```
        Translation profile (Outgoing):
        incoming call blocking:
        translation-profile = `'
        disconnect-cause = `no-service'
voice-port = `'
        type = pots, prefix = `',
        forward-digits default
        session-target = `', up,
        direct-inward-dial = disabled,
        digit_strip = enabled,
        register E.164 number with GK = TRUE
        fax rate = system,   payload size =  20 bytes
        Time elapsed since last clearing of voice call statistics never
        Connect Time = 0, Charged Units = 0,
        Successful Calls = 0, Failed Calls = 0, Incomplete Calls = 0
        Accepted Calls = 0, Refused Calls = 0,
        Last Disconnect Cause is "",
        Last Disconnect Text is "",
        Last Setup Time = 0.
Matched:   Digits:0
Target:
```

Related Commands

Command	Description
show dialplan dialpeer	Displays which outbound dial peer is matched based upon the incoming dialed number and the COR criteria specified in the command line.
show dialplan in-carrier	Displays which VoIP or POTS dial peer is matched for a specific source carrier.
show dialplan incall	Displays which POTS dial peer is matched for a specific calling number or voice port.
show dialplan number	Displays which dial peer is matched for a particular telephone number.

show dialplan number

To display which outgoing dial peer is reached when a particular telephone number is dialed, use the **show dialplan number** command in privileged EXEC mode.

show dialplan number *dial-string* [**carrier identifier**] [**fax** | **huntstop** | **voice**] [**timeout**]

Syntax Description

dial -string	Particular destination pattern (E.164 telephone number).
carrier	(Optional) Indicates that you wish to base your search for applicable dial peers on the source carrier identifier.
identifier	(Optional) Source carrier identifier to accompany the **carrier** keyword.
fax	(Optional) Fax information type.
huntstop	(Optional) Terminates further dial-peer hunting upon encountering the first dial-string match.
timeout	(Optional) Allows matching for variable-length destination patterns.
voice	(Optional) Voice information type.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
11.3(1)T	This command was introduced on the Cisco 3600 series.
12.2(1)	The **huntstop** keyword was added.
12.2(8)T	This command was implemented on the Cisco 1751, Cisco 2600 series, Cisco 3725, and Cisco 3745 and the timeout keyword was added.
12.2(11)T	The **carrier**, **fax**, and **voice** keywords were added.

Usage Guidelines

Use this command to test whether the dial plan configuration is valid and working as expected. Use the timeout keyword to enable matching variable-length destination patters associated with dial peers. This can increase you r chances of finding a match for the dial peer number you specify.

Examples

The following is sample output from thiscommand using a destination pattern of 1001:

```
Router# show dialplan number 1001
Macro Exp.: 1001
VoiceEncapPeer1003
        information type = voice,
        tag = 1003, destination-pattern = `1001',
        answer-address = `', preference=0,
        numbering Type = `unknown'
        group = 1003, Admin state is up, Operation state is up,
        incoming called-number = `', connections/maximum = 0/unlimited,
```

```
         DTMF Relay = disabled,
         huntstop = enabled,
         type = pots, prefix = `',
         forward-digits default
         session-target = `', voice-port = `1/1',
         direct-inward-dial = disabled,
         Connect Time = 0, Charged Units = 0,
         Successful Calls = 0, Failed Calls = 0, Incomplete Calls = 0
         Accepted Calls = 0, Refused Calls = 0,
         Last Disconnect Cause is "",
         Last Disconnect Text is "",
         Last Setup Time = 0.
Matched: 1001   Digits: 4
Target:
VoiceEncapPeer1004
         information type = voice,
         tag = 1004, destination-pattern = `1001',
         answer-address = `', preference=0,
         numbering Type = `unknown'
         group = 1004, Admin state is up, Operation state is up,
...
Matched: 1001   Digits: 4
Target:
VoiceEncapPeer1002
         information type = voice,
         tag = 1002, destination-pattern = `1001',
         answer-address = `', preference=0,
         numbering Type = `unknown'
         group = 1002, Admin state is up, Operation state is up,
...
Matched: 1001   Digits: 4
Target:
VoiceEncapPeer1001
         information type = voice,
         tag = 1001, destination-pattern = `1001',
         answer-address = `', preference=0,
         numbering Type = `unknown'
         group = 1001, Admin state is up, Operation state is up,
...
Matched: 1001   Digits: 4
Target:
```

The following is sample output from this command using a destination pattern of 1001 and the **huntstop** keyword:

```
Router# show dialplan number 1001 huntstop
 Macro Exp.: 1001
 VoiceEncapPeer1003
         information type = voice,
         tag = 1003, destination-pattern = `1001',
         answer-address = `', preference=0,
         numbering Type = `unknown'
         group = 1003, Admin state is up, Operation state is up,
         incoming called-number = `', connections/maximum = 0/unlimited,
         DTMF Relay = disabled,
         huntstop = enabled,
         type = pots, prefix = `',
         forward-digits default
         session-target = `', voice-port = `1/1',
         direct-inward-dial = disabled,
         Connect Time = 0, Charged Units = 0,
         Successful Calls = 0, Failed Calls = 0, Incomplete Calls = 0
         Accepted Calls = 0, Refused Calls = 0,
```

```
        Last Disconnect Cause is "",
        Last Disconnect Text is "",
        Last Setup Time = 0.
Matched: 1001   Digits: 4
Target:
```

Related Commands

Command	Description
show dialplan dialpeer	Displays which outbound dial peer is matched based upon the incoming dialed number and the COR criteria specified in the command line.
show dialplan incall	Displays which POTS dial peer is matched for a specific calling number or voice port.
show dialplan in-carrier	Displays which VoIP or POTS dial peer is matched for a specific source carrier.
show dialplan in-trunk-group-label	Displays which VoIP or POTS dial peer is matched for a specific source trunk group.

show dialplan uri

To display which outbound dial peer is matched for a specific destination uniform resource identifier (URI), use the **show dialplan uri**command in privileged EXEC mode.

show dialplan uri *uri*

Syntax Description

uri	Destination Session Initiation Protocol (SIP) or telephone (TEL) URI for the outgoing call.

Command Default

No default behavior or values

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.3(4)T	This command was introduced.

Usage Guidelines

- Use this command for troubleshooting to determine which dial peer is matched for an outgoing call, based on the selected URI.
- To set the URI format used to match calls, use the **voice class uri** command. To set the URI voice class in the outbound dial peer, use the **destination uri** command.

Examples

The following is sample output from this command:

```
Router# show dialplan uri sip:123456
 Outbound dialpeer matching based on destination URI
VoiceOverIpPeer99
        peer type = voice, information type = voice,
        description = `',
        tag = 99, destination-pattern = `',
        answer-address = `', preference=0,
        CLID Restriction = None
        CLID Network Number = `'
        CLID Second Number sent
        source carrier-id = `', target carrier-id = `',
        source trunk-group-label = `',  target trunk-group-label = `',
        numbering Type = `unknown'
        group = 99, Admin state is up, Operation state is up,
        incoming called-number = `', connections/maximum = 0/unlimited,
        DTMF Relay = disabled,
        modem transport = system,
        URI classes:
            Incoming (Request) =
            Incoming (To) =
            Incoming (From) =
            Destination = 100
        huntstop = disabled,
        in bound application associated: 'DEFAULT'
        out bound application associated: ''
        dnis-map =
        permission :both
```

```
        incoming COR list:maximum capability
        outgoing COR list:minimum requirement
        Translation profile (Incoming):
        Translation profile (Outgoing):
        incoming call blocking:
        translation-profile = `'
        disconnect-cause = `no-service'
        type = voip, session-target = `',
        technology prefix:
        settle-call = disabled
        ip media DSCP = ef, ip signaling DSCP = af31, UDP checksum = disabled,
        session-protocol = sipv2, session-transport = system, req-qos = best-ef
        acc-qos = best-effort,
        RTP dynamic payload type values: NTE = 101
        Cisco: NSE=100, fax=96, fax-ack=97, dtmf=121, fax-relay=122
               CAS=123, ClearChan=125, PCM switch over u-law=0,A-law=8
        RTP comfort noise payload type = 19
        fax rate = voice,   payload size =  20 bytes
        fax protocol = system
        fax-relay ecm enable
        fax NSF = 0xAD0051 (default)
        codec = g729r8,   payload size =  20 bytes,
        Expect factor = 0, Icpif = 20,
        Playout Mode is set to default,
        Initial 60 ms, Max 300 ms
        Playout-delay Minimum mode is set to default, value 40 ms
        Fax nominal 300 ms
        Max Redirects = 1, signaling-type = ext-signal,
        VAD = enabled, Poor QOV Trap = disabled,
        Source Interface = NONE
        voice class sip url = system,
        voice class sip rel1xx = system,
        voice class perm tag = `'
        Time elapsed since last clearing of voice call statistics never
        Connect Time = 0, Charged Units = 0,
        Successful Calls = 0, Failed Calls = 0, Incomplete Calls = 0
        Accepted Calls = 0, Refused Calls = 0,
        Last Disconnect Cause is "",
        Last Disconnect Text is "",
        Last Setup Time = 0.
Matched:    Digits: 0
Target:
```

Related Commands

Command	Description
debug voice uri	Displays debugging messages related to URI voice classes.
destination uri	Specifies the voice class used to match the dial peer to the destination URI for an outgoing call.
show dialplan incall uri	Displays which dial peer is matched for a specific URI in an incoming call.
voice class uri	Creates or modifies a voice class for matching dial peers to a SIP or TEL URI.
voice class uri sip preference	Sets a preference for selecting voice classes for a SIP URI.

show dn-numbers

To display directory number information of Call Manager Express (CME), use the **show dn-numbers** command in user EXEC or privileged EXEC mode.

show dn-numbers

Syntax Description

This command has no arguments or keywords.

Command Modes

User EXEC (>)
Privileged EXEC (#))

Command History

Release	Modification
12.4(15)T	This command was introduced.
Cisco IOS XE Release 2.4	This command was integrated into Cisco IOS XE Release 2.4.

Examples

The following is sample output from the **show dn-numbers** command:

```
Router# show dn-numbers

 Directory numbers
 Entry          name                          number
 1              user1                         0
 10             user2                         7890
 3              user3                         1234
 4              user4                         890
 12             user5                         5676
 11             user6                         987

 ephone directory numbers
 DN             name                           number
 2              user7                          1000
 4              user10                         34567
 6              user11                         1234567891
 10             user12                         1234567
sip phone numbers
 DN             name                           number
 1              user13                         10000
 8              user14                         87953893
 9              user15                         Not Configured
```

The table below describes the significant fields shown in the display.

Table 69: show dn-numbers Field Descriptions

Field	Description
DN	Directory number.
name	Name of the connection.

Field	Description
number	Telephone number.

show dspfarm

To display digital signal processor (DSP) farm service information such as operational status and DSP resource allocation for transcoding and conferencing, use the **show dspfarm** command in user EXEC or privileged EXEC mode.

show dspfarm [**all** | **dsp** { **active** | **all** | **idle** | **stats** *bridge-id* [**sample** *seconds*] } | **profile** [*profile-id*] | **sessions** [*session-id*] | **video** { **conference** | **statistics** | **transcode** }]

Cisco ASR 1000 Series Router
show dspfarm { **all** | **dsp** { **active** | **all** | **idle** | **stats** *bridge-id* [**sample** *seconds*] } | **profile** [*profile-identifier*] }

Syntax Description

all	(Optional) Displays all global information about the DSP farm service.
dsp	(Optional) Displays DSP information about the DSP farm service.
active	Displays active DSP information about the DSP farm service.
all	Displays all DSP information about the DSP farm service.
idle	Displays idle DSP information about the DSP farm service.
stats	Displays DSP statistics about the DSP farm service.
bridge-id	Displays the DSP statistics for a call bridge the specified bridge ID.
sample	(Optional) Displays statistics of the specified sample interval.
seconds	(Optional) The DSP sample interval time, in seconds.
profile	(Optional) Displays profiles about the DSP farm service.
profile-id	(Optional) The profile ID about the DSP farm service.
sessions	(Optional) Displays sessions and connections about the DSP farm service.
session-id	(Optional) The session identifier to be displayed for the DSP farm service.
video	(Optional) Displays information on video resources.
conference	(Optional) Displays the DSP information, such as the codecs, video bridge channel, and transmit (tx) and receive (rx) packets that are used for each participant in a conference and is grouped by conference sessions.
statistics	(Optional) Displays the DSP statistics of the call bridge.
transcode	(Optional) Displays the DSP status and statistics for the transcoding call.

Command Modes

User EXEC (>)

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE 17.18.2	This command was implemented on C8375-E-G2 router platform.
15.1(4)M	This command was modified. The **video**, **conference**, **statistics**, and **transcode** keywords were added.
Cisco IOS XE Release 3.2S	This command was implemented on the Cisco ASR 1000 Series Router.
12.4(15)T	The **stats**, **sample**, **sessions**, and **profile** keywords were added. The *bridge-id*, *profile-id*, *seconds*, and *session-id* arguments were added.
12.2(13)T	This command was implemented on the Cisco 2600 series, Cisco 3620, Cisco 3640, Cisco 3660, and Cisco 3700 series.
12.1(5)YH	This command was introduced on the Cisco VG200.

Usage Guidelines

The router on which this command is used must be equipped with one or more digital T1/E1 packet voice trunk network modules (NM-HDVs) or high-density voice (HDV) transcoding/conferencing DSP farms (NM-HDV-FARMs) to provide DSP resources.

Cisco ASR 1000 Series Router

The show dspfarm command is used to view the DSP farm service information such as operational status and DSP resource allocation for transcoding.

Note The **session** keyword and *session-id* argument is not supported on Cisco ASR 1000 Series Router.

Examples

The following is sample output from several forms of the **show dspfarm** command. The fields are self explanatory.

```
Router# show dspfarm
DSPFARM Configuration Information:
Admin State: UP, Oper Status: ACTIVE - Cause code: NONE
Transcoding Sessions: 4, Conferencing Sessions: 0
RTP Timeout: 600
Router# show dspfarm all
DSPFARM Configuration Information:
Admin State: UP, Oper Status: ACTIVE - Cause code: NONE
Transcoding Sessions: 4, Conferencing Sessions: 2
RTP Timeout: 1200
Connection average duration: 3600, Connection check interval 600
Codec G729 VAD: ENABLED
Total number of active session(s) 0, and connection(s) 0
SLOT  DSP   CHNL  STATUS USE   TYPE   SESS-ID   CONN-ID   PKTS-RXED PKTS-TXED
1     3     1     UP     FREE  conf   -         -         -         -
1     3     2     UP     FREE  conf   -         -         -         -
1     3     3     UP     FREE  conf   -         -         -         -
1     3     4     UP     FREE  conf   -         -         -         -
1     3     5     UP     FREE  conf   -         -         -         -
1     3     6     UP     FREE  conf   -         -         -         -
1     4     1     UP     FREE  conf   -         -         -         -
1     4     2     UP     FREE  conf   -         -         -         -
1     4     3     UP     FREE  conf   -         -         -         -
```

```
1     4     4     UP     FREE  conf   -         -         -         -
1     4     5     UP     FREE  conf   -         -         -         -
1     4     6     UP     FREE  conf   -         -         -         -
1     5     1     UP     FREE  xcode  -         -         -         -
1     5     2     UP     FREE  xcode  -         -         -         -
1     5     3     UP     FREE  xcode  -         -         -         -
1     5     4     UP     FREE  xcode  -         -         -         -
1     5     5     UP     FREE  xcode  -         -         -         -
1     5     6     UP     FREE  xcode  -         -         -         -
1     5     7     UP     FREE  xcode  -         -         -         -
1     5     8     UP     FREE  xcode  -         -         -         -
Total number of DSPFARM DSP channel(s) 20
Router# show dspfarm dsp all
DSPFARM Configuration Information:
Admin State: UP, Oper Status: ACTIVE - Cause code: NONE
Transcoding Sessions: 4, Conferencing Sessions: 2
RTP Timeout: 1200
Connection average duration: 3600, Connection check interval 600
Codec G729 VAD: ENABLED
Total number of active session(s) 0, and connection(s) 0
SLOT  DSP  CHNL  STATUS  USE   TYPE   SESS-ID  CONN-ID  PKTS-RXED  PKTS-TXED
1     3    1     UP      FREE  conf   -        -        -          -
1     3    2     UP      FREE  conf   -        -        -          -
1     3    3     UP      FREE  conf   -        -        -          -
1     3    4     UP      FREE  conf   -        -        -          -
1     3    5     UP      FREE  conf   -        -        -          -
1     3    6     UP      FREE  conf   -        -        -          -
1     4    1     UP      FREE  conf   -        -        -          -
1     4    2     UP      FREE  conf   -        -        -          -
1     4    3     UP      FREE  conf   -        -        -          -
1     4    4     UP      FREE  conf   -        -        -          -
1     4    5     UP      FREE  conf   -        -        -          -
1     4    6     UP      FREE  conf   -        -        -          -
1     5    1     UP      FREE  xcode  -        -        -          -
1     5    2     UP      FREE  xcode  -        -        -          -
1     5    3     UP      FREE  xcode  -        -        -          -
1     5    4     UP      FREE  xcode  -        -        -          -
1     5    5     UP      FREE  xcode  -        -        -          -
1     5    6     UP      FREE  xcode  -        -        -          -
1     5    7     UP      FREE  xcode  -        -        -          -
1     5    8     UP      FREE  xcode  -        -        -          -
Total number of DSPFARM DSP channel(s) 20



Router# show dspfarm sessions
sess_id  conn_id  stype  mode      codec  pkt  ripaddr      rport  sport
4        145      xcode  sendrecv  g711a  20   10.10.10.19  19460  21284
4        161      xcode  sendrecv  g729   10   10.10.10.28  19414  20382
5        177      xcode  sendrecv  g711u  20   10.10.10.17  18290  21170
5        193      xcode  sendrecv  g729b  10   10.10.10.18  19150  18968
```

The following output shows the active channels on the slots of C8375-E-G2 router platform:

```
Router# show dspfarm dsp active

    VDSP   DSP VERSION  STATUS CHNL USE   TYPE    RSC_ID BRIDGE_ID PKTS_TXED PKTS_RXED

     vDSP   1   1.0.827  UP     4    USED  xcode   1      24        0         0
     vDSP   1   1.0.827  UP     4    USED  xcode   1      23        0         0
        Total number of DSPFARM DSP channel(s) 1
```

Examples

The following sample output displays dspfarm profiles for video conferencing and video transcoding:

```
Router# show dspfarm profile
 Profile ID = 1, Service = VIDEO CONFERENCING, Resource ID = 2
 Video Conference Type : HOMOGENEOUS, Layout : disabled
 Profile Description :
 Profile Service Mode : Non Secure
 Profile Admin State : DOWN
 Profile Operation State : DOWN
 Application : SCCP   Status : NOT ASSOCIATED
 Resource Provider : FLEX_DSPRM   Status : NONE
 Number of Resource Configured : 1
 Number of Resource Available : 0
 Maximum conference participants : 16
 Codec Configuration: num_of_codecs:6
 Codec : g711ulaw, Maximum Packetization Period : 30
 Codec : g711alaw, Maximum Packetization Period : 30
 Codec : g729ar8, Maximum Packetization Period : 60
 Codec : g729abr8, Maximum Packetization Period : 60
 Codec : g729r8, Maximum Packetization Period : 60
 Codec : g729br8, Maximum Packetization Period : 60
 Video Codec Configuration:
 Codec : h263
   Resolution : cif
     Frame rate:30, Min bitrate:320kbps, Max bitrate:320kbps
     Payload protocol : rfc-2190, Extension : annex-none
 Profile ID = 2, Service = VIDEO CONFERENCING, Resource ID = 3
 Video Conference Type : HETEROGENEOUS, Layout : disabled
 Profile Description :
 Profile Service Mode : Non Secure
 Profile Admin State : UP
 Profile Operation State : ACTIVE IN PROGRESS
 Application : SCCP   Status : ASSOCIATION IN PROGRESS
 Resource Provider : FLEX_DSPRM   Status : UP
 Number of Resource Configured : 1
 Number of Resource Available : 1
 Maximum conference participants : 4
 Maximum video ports : 4
 Codec Configuration: num_of_codecs:6
 Codec : g729br8, Maximum Packetization Period : 60
 Codec : g729r8, Maximum Packetization Period : 60
 Codec : g729abr8, Maximum Packetization Period : 60
 Codec : g729ar8, Maximum Packetization Period : 60
 Codec : g711alaw, Maximum Packetization Period : 30
 Codec : g711ulaw, Maximum Packetization Period : 30
 Video Codec Configuration:
 Codec : h264
   Resolution : qcif
     Frame rate:15, Min bitrate:64kbps, Max bitrate:704kbps
     Frame rate:30, Min bitrate:64kbps, Max bitrate:704kbps
   Resolution : cif
     Frame rate:15, Min bitrate:64kbps, Max bitrate:704kbps
     Frame rate:30, Min bitrate:64kbps, Max bitrate:704kbps
 Codec : h263
   Resolution : qcif
     Frame rate:15, Min bitrate:64kbps, Max bitrate:704kbps
     Frame rate:30, Min bitrate:64kbps, Max bitrate:704kbps
   Resolution : cif
     Frame rate:15, Min bitrate:64kbps, Max bitrate:704kbps
     Frame rate:30, Min bitrate:64kbps, Max bitrate:704kbps
Dspfarm Profile Configuration
Profile ID = 3, Service =Universal TRANSCODING, Resource ID = 1
 Profile Description :
```

```
 Profile Service Mode : Non Secure
 Profile Admin State : DOWN
 Profile Operation State : DOWN
 Application : SCCP   Status : NOT ASSOCIATED
 Resource Provider : FLEX_DSPRM   Status : NONE
 Number of Resource Configured : 0
 Number of Resource Available : 0
 Codec Configuration: num_of_codecs:4
 Codec : g711ulaw, Maximum Packetization Period : 30
 Codec : g711alaw, Maximum Packetization Period : 30
 Codec : g729ar8, Maximum Packetization Period : 60
 Codec : g729abr8, Maximum Packetization Period : 60
```

Examples

The following sample output displays DSP information for video conferences:

```
Router# show dspfarm video conference
 VIDEO CONFERENCE SESSION: slot 0 dsp 3 channel_id 1 rsc_id 8 profile_id 101
 conferee_id 1  name_num:  62783363
         audio_codec g711u     pkt_size 160  bridge_id 1
         dsp_txed_pkts 25993     dsp_rxed_pkts 25888
 conferee_id 1  name_num:  62783363
         video_codec H264_VGA  rfc_number RFC3984 payload rx: 97   tx:97
         framerate 30 bitrate(k) 960  annex 0x40
         cluster_id 0  bridge_id 2         layout_id 0
         dsp_txed_pkts 59230     dsp_rxed_pkts 63019
 conferee_id 2  name_num:  62783365
         audio_codec g711u     pkt_size 160  bridge_id 3
         dsp_txed_pkts 21682     dsp_rxed_pkts 21598
 conferee_id 2  name_num:  62783365
         video_codec H264_4CIF rfc_number RFC3984 payload rx: 97   tx:97
         framerate 30 bitrate(k) 960  annex 0x40
         cluster_id 1  bridge_id 4         layout_id 0
         dsp_txed_pkts 49488     dsp_rxed_pkts 78510
 conferee_id 3  name_num:  3004
         audio_codec g711u     pkt_size 160  bridge_id 5
         dsp_txed_pkts 12130     dsp_rxed_pkts 12067
 conferee_id 3  name_num:  3004
         video_codec H264_CIF  rfc_number RFC3984 payload rx: 97   tx:97
         framerate 30 bitrate(k) 704  annex 0x40
         cluster_id 2  bridge_id 6         layout_id 0
         dsp_txed_pkts 20354     dsp_rxed_pkts 25702
 conferee_id 4  name_num: LifeSize LifeSize
         audio_codec g711u     pkt_size 160  bridge_id 7
         dsp_txed_pkts 1751      dsp_rxed_pkts 1672
 conferee_id 4  name_num: LifeSize LifeSize
         video_codec H264_4CIF rfc_number RFC3984 payload rx: 96   tx:96
         framerate 30 bitrate(k) 1100 annex 0x40
         cluster_id 1  bridge_id 8         layout_id 0
         dsp_txed_pkts 3558      dsp_rxed_pkts 3569
 cluster_id 0  video_codec H264_VGA  rfc_number RFC3984 rfc_payload 100
         framerate 30 bitrate(k) 1000, annex 0x40
 decoder_id 1  slot 0  dsp 13 codec h264 vga           cluster_id 0
 encoder_id 1  slot 0  dsp 10 codec h264 vga           cluster_id 0
 cluster_id 1  video_codec H264_4CIF rfc_number RFC3984 rfc_payload 100
         framerate 30 bitrate(k) 1000, annex 0x40
 decoder_id 1  slot 0  dsp 2  codec h264 4cif          cluster_id 1
 encoder_id 1  slot 0  dsp 7  codec h264 4cif          cluster_id 1
 cluster_id 2  video_codec H264_CIF  rfc_number RFC3984 rfc_payload 100
         framerate 30 bitrate(k) 704 , annex 0x40
 decoder_id 1  slot 0  dsp 15 codec h264 cif           cluster_id 2
 encoder_id 1  slot 0  dsp 14 codec h264 cif           cluster_id 2
Total number of DSPFARM DSP channel(s) 1
```

Examples

The following sample output displays the statistics for a call that uses video transcoding:

```
Router#  show dspfarm dsp stats
Gathering total stats...
Video Statistics for bridge_id=3 call_id=2
 Video Decoder Statistics:
  Slot=0  DSP_Id=8  Decoder_Id=1
  CallDuration=268  Codec=1  ProfileId=0x0  LevelId=0
  PicWidth=352  PicHeight=288  FrameRate=30  Bitrate=360000
  NumMacroBlocksConcealed=0  NumFramesConcealed=0
  NumPackets=13269  NumBytesConsumed=12096254
  NumBadHeaderPackets=0  NumOutOfSyncPackets=24
  NumBufferOverflow=0
 Video Encoder Statistics:
  Slot=0  DSP_Id=2  Encoder_Id=1
  Duration=268  Codec=1  ProfileId=0x0  LevelId=0
  PicWidth=176  PicHeight=144  FrameRate=30  Bitrate=704000
  InstantBitrate=440000  NumPackets=17571  NumBytesGenerated=14830996
```

Examples

The following sample output displays the statistics for a video conference:

```
Router# show dspfarm dsp stats
Gathering total stats...
Video Statistics for bridge_id=3 call_id=4
 Video Conferee Status - ConfereeID=1
  ContributionState=0x1  IngressMute=0  EgressMute=0
  DtmfRtpPlt=0  ClusterId=1  StreamDir=3
  PayloadType=0x6161  TxSSRC=0x1F3C  RtpProtocol=2
  CodecType=2  Annex=0x0  PicWidth=352  PicHeight=288
  FrameRate=30  Bitrate(x100)=3760
 Video Conferee Statistics - ConfereeID=1
  TotalRxPackets=5076  TotalRxBytes=3957126
  TotalTxPackets=3829  TotalTxBytes=3429797
  TotalDroppedPackets=3  CurDroppedPackets=0
  TotalOutOfOrderPackets=0  CurOutOfOrderPackets=0
  MaxObservedJitter=0  CurObservedJitter=0
  MaxObservedDelay=0  CurObservedDelay=0
  MaxOutOfSyncDelay=0  CurOutOfSyncDelay=0
  ActualFrameRate=0  ActualBitrate(x100)=2017
  FastVideoUpdateRate=0  TotalDuration=135
 Video Conference Status:
  ServiceType=0  MuteAllStatus=0
  CurSpeakerConfereeId=1  LastSpeakerConfereeId=3  NewSpeakerConfereeId=0
  ConfereeIdBitMap=0x07
 Video Conference Statistics:
  NumActiveChans=3  NumMaxChans=1
  TotalRxPackets=42589  TotalRxBytes=29979147
  TotalTxPackets=12361  TotalTxBytes=10003701
  TotalDroppedPackets=3  CurDroppedPackets=0
  TotalOutOfOrderPackets=0  CurOutOfOrderPackets=0
  MaxObservedJitter=0  CurObservedJitter=0
  MaxObservedDelay=0  CurObservedDelay=0
MaxOutOfSyncDelay=0  CurOutOfSyncDelay=0
```

Examples

The following is a sample output of the **show dspfarm** all command on Cisco ASR 1000 Series Router:

```
Router# show dspfarm all
Dspfarm Profile Configuration
 Profile ID = 1, Service = TRANSCODING, Resource ID = 1
 Profile Description :
 Profile Service Mode : Non Secure
 Profile Admin State : UP
 Profile Operation State : ACTIVE
 Application : SBC   Status : ASSOCIATED
 Resource Provider : FLEX_DSPRM   Status : UP
 Number of Resources Configured : 588
 Number of Resources Out of Service : 0
 Codec Configuration
 Codec : g711ulaw, Maximum Packetization Period : 30
 Codec : g711alaw, Maximum Packetization Period : 30
 Codec : g729ar8, Maximum Packetization Period : 60
 Codec : g729abr8, Maximum Packetization Period : 60
SLOT DSP VERSION  STATUS CHNL USE   TYPE    RSC_ID BRIDGE_ID
5    1   26.7.0   UP     N/A  FREE  xcode  1      -         -         -
5    1   26.7.0   UP     N/A  FREE  xcode  1      -         -         -
5    1   26.7.0   UP     N/A  FREE  xcode  1      -         -         -
5    1   26.7.0   UP     N/A  FREE  xcode  1      -         -         -
5    1   26.7.0   UP     N/A  FREE  xcode  1      -         -         -
```

The following is a sample output of the **show dspfarm dsp idle** command providing idle DSP information on Cisco ASR 1000 Series Router:

```
Router# show dspfarm dsp idle
SLOT DSP VERSION  STATUS CHNL USE   TYPE    RSC_ID BRIDGE_ID
5    1   26.7.0   UP     N/A  FREE  xcode  1      -         -         -
5    1   26.7.0   UP     N/A  FREE  xcode  1      -         -         -
5    1   26.7.0   UP     N/A  FREE  xcode  1      -         -         -
5    1   26.7.0   UP     N/A  FREE  xcode  1      -         -         -
5    1   26.7.0   UP     N/A  FREE  xcode  1      -         -         -
5    1   26.7.0   UP     N/A  FREE  xcode  1      -         -         -
5    1   26.7.0   UP     N/A  FREE  xcode  1      -         -         -
5    1   26.7.0   UP     N/A  FREE  xcode  1      -         -         -
5    1   26.7.0   UP     N/A  FREE  xcode  1      -         -         -
```

The following is sample output of the **show dspfarm profile 1** command providing DSP Farm profile configuration details such as application association, number of resources configured, Codecs added, and maximum number of sessions for profile 1 on Cisco ASR 1000 Series Router.

```
Router# show dspfarm profile 1
Dspfarm Profile Configuration
 Profile ID = 1, Service = TRANSCODING, Resource ID = 1
 Profile Description :
 Profile Service Mode : Non Secure
 Profile Admin State : UP
 Profile Operation State : ACTIVE
 Application : SBC   Status : ASSOCIATED
 Resource Provider : FLEX_DSPRM   Status : UP
 Number of Resources Configured : 588
 Number of Resources Out of Service : 0
 Codec Configuration
 Codec : g711ulaw, Maximum Packetization Period : 30
 Codec : g711alaw, Maximum Packetization Period : 30
 Codec : g729ar8, Maximum Packetization Period : 60
 Codec : g729abr8, Maximum Packetization Period : 60
```

```
Router#show dspfarm profile ?
  <1-65535>  Profile ID
  |          Output modifiers
  <cr>
```

Related Commands

Command	Description
dspfarm (DSP farm)	Enables DSP-farm service.

show dspfarm profile

To display configured digital signal processor (DSP) farm profile information for a selected Cisco CallManager group, use the **show dspfarm profile**command in privileged EXEC mode.

show dspfarm profile [*profile-identifier*]

Syntax Description

profile ide ntifier	(Optional) Number that uniquely identifies a profile. Range is from 1 to 65535. There is no default.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.3(8)T	This command was introduced.

Usage Guidelines

Use the **show dspfarm profile** command to verify that the association between Skinny Client Control Protocol (SCCP) Cisco Unified CallManager and the DSP farm profiles match your organizational plan.

The output of the **show dspfarm profile** command differs depending on the services configured in the profile.

Examples

```
The following is sample output from the show dspfarm profile
 command:
Router# show dspfarm profile

Dspfarm Profile Configuration
 Profile ID = 6, Service = TRANSCODING, Resource ID = 1
 Profile Description :
 Profile Service Mode : Non Secure
 Profile Admin State : UP
 Profile Operation State : ACTIVE
 Application : SCCP   Status : ASSOCIATED
 Resource Provider : FLEX_DSPRM   Status : UP
 Number of Resource Configured : 4
 Number of Resource Available : 4
 Codec Configuration
 Codec : g711ulaw, Maximum Packetization Period : 30
 Codec : g711alaw, Maximum Packetization Period : 30
 Codec : g729ar8, Maximum Packetization Period : 60
 Codec : g729abr8, Maximum Packetization Period : 60
 Codec : g729br8, Maximum Packetization Period : 60
 RSVP : ENABLED
 TRP : FW-TRAVERSAL ENABLED
Dspfarm Profile Configuration
 Profile ID = 27, Service = CONFERENCING, Resource ID = 2
 Profile Description :
 Profile Service Mode : Non Secure
 Profile Admin State : UP
 Profile Operation State : ACTIVE
 Application : SCCP   Status : ASSOCIATED
 Resource Provider : FLEX_DSPRM   Status : UP
 Number of Resource Configured : 6
 Number of Resource Available : 6
```

```
 Codec Configuration
 Codec : g711alaw, Maximum Packetization Period : 30
 Codec : g729ar8, Maximum Packetization Period : 60
Dspfarm Profile Configuration
 Profile ID = 34, Service = MTP, Resource ID = 1
 Profile Description :
 Profile Service Mode : secure
 Profile Admin State : UP
 Profile Operation State : ACTIVE
 Application : SCCP   Status : ASSOCIATED
 Resource Provider : NONE   Status : UP
 Number of Resource Configured : 2
 Number of Resource Available : 2
 Hardware Configured Resources : 1
 Hardware Available Resources : 1
 Software Resources : 1
 Codec Configuration
 Codec : g711ulaw, Maximum Packetization Period : 30
 TRP : FW-TRAVERSAL ENABLED
```

The table below describes the significant fields shown in the display.

Table 70: show dspfarm profile Field Descriptions

Field	Description
Profile ID	Displays the profile ID number.
Service	Displays the service that is associated with the profile.
Resource ID	Displays the ID number that the profile is associated with in the Cisco CallManager register.
Profile Description	Displays the description of the profile.
Profile Service Mode	The status of the profile service. It can be either Secure or Non Secure.
Profile Admin State	Displays the status of the profile. If the Profile Admin State is DOWN, use the **no shutdown** command in DSP farm profile configuration mode.
Profile Operation State	Displays the status of the DSP farm profiles registration process with the Cisco CallManager. Status options are as follows: • ACTIVE--The profile is registered with the Cisco Unified CallManager. • ACTIVE IN PROGRESS--The profile is still registering with the Cisco Unified CallManager. Wait for the profile to finish registering. • DOWN--The profile is not registering with the Cisco Unified CallManager. Check the connectivity between the DSP farm gateway and the Cisco Unified CallManager. • DOWN IN PROGRESS--The profile is deregistering from the Cisco Unified CallManager and deallocating the DSP resources. • RESOURCE ALLOCATED--The DSP resources for this profile are allocated or reserved.

Field	Description
Application	Displays the routing protocol used.
Number of Resource Configured	Maximum number of sessions that are supported by a profile.
Number of Resource Available	Total number of resources that are configurable.
Hardware Configured Resources	Number of sessions configured in the profile.
Hardware Available Resources	Number of sessions available for this profile.
Software Resources	Number of software sessions configured for this profile (applicable only to MTP profiles).
Codec Configuration	Lists the codecs that are configured. **Note** Media Termination Point (MTP) profile supports only one codec per profile.
RSVP	Resource Reservation Protocol (RSVP) support for this profile.
TRP	Displays whether firewall traversal is enabled for Trusted Relay Point.

Related Commands

Command	Description
dsp services dspfarm	Configures DSP farm services for a specified voice card.
dspfarm profile	Enters DSP farm profile configuration mode and defines a profile for DSP farm services.
show media resource status	Displays the current media resource status.

show dsp-group

To display digital signal processor (DSP) group information including both voice and video information, use the **show dsp-group** command in user EXEC or privileged EXEC mode.

show dsp-group {**all** | **slot** *slot-number* | **video** [**all** | **slot** *slot-number*] | **voice** [**all** | **slot** *slot-number*]}

Syntax Description

all	Displays DSP information for all DSP group.
slot	Displays DSP information for the specified slot.
slot-number	Slot used in the DSP group.
video	Displays information on video resources.
voice	Displays information on voice resources.

Command Modes

User EXEC (>)
Privileged EXEC (#)

Command History

Release	Modification
15.1(4)M	This command was introduced.

Usage Guidelines

The router on which this command is used must be equipped with one or more digital T1/E1 packet voice trunk network modules (NM-HDVs), high-density voice (HDV) transcoding/conferencing DSP farms (NM-HDV-FARMs), or packet voice data module (PVDM) slots to provide DSP resources.

Examples

The following shows sample output from several forms of the **show dsp-group**command. The fields are self explanatory.

```
Router# show dsp-group all
DSP groups on slot 0:
dsp 1:
  State: UP, firmware: 28.0.103
  Max signal/voice channel: 32/32
  Max credits: 480, Voice credits: 0, Video credits: 480
  num_of_sig_chnls_allocated: 32
  Transcoding channels allocated: 0
  Group: FLEX_GROUP_VIDEO_POOL, complexity: FLEX
    Video Credits Max: 480, Share: 0, Reserved (rounded-up): 480
    Video Group: VIDEO_CONF, rsc id: 2, mode: VCONF_HETE
      Session: 0, maximum participants: 4
        Video Transcoding channels reserved credits: 480
        Video Transcoding channels allocated: 1
          Encoder: inactive, credit reserved: 480
  Slot: 0
  Device idx: 0
  PVDM Slot: 0
  Dsp Type: SP2600
dsp 2:
```

```
  State: UP, firmware: 28.0.103
  Max signal/voice channel: 32/32
  Max credits: 480, Voice credits: 0, Video credits: 480
  num_of_sig_chnls_allocated: 32
  Transcoding channels allocated: 0
  Group: FLEX_GROUP_VIDEO_POOL, complexity: FLEX
    Video Credits Max: 480, Share: 0, Reserved (rounded-up): 480
    Video Group: VIDEO_CONF, rsc id: 2, mode: VCONF_HETE
      Session: 0, maximum participants: 4
        Video Transcoding channels reserved credits: 480
        Video Transcoding channels allocated: 3
          Decoder: inactive, credits reserved: 160
          Decoder: inactive, credits reserved: 160
          Decoder: inactive, credits reserved: 160
  Slot: 0
  Device idx: 0
  PVDM Slot: 0
  Dsp Type: SP2600
DSP groups on slot 1:
 This command is not applicable to slot 1
DSP groups on slot 2:
 This command is not applicable to slot 2
DSP groups on slot 3:
 This command is not applicable to slot 3
```

Related Commands

Command	Description
dsp service dspfarm	Configures DSP farm services for a specified voice card.
dspfarm (DSP farm)	Enables DSP-farm service.
voice service dsp-reservation	Configures the percentage of DSP resources are reserved for voice services and enables video services to use the remaining DSP resources. This command is required to enable video services.
voice-card	Enters voice-card configuration mode.

show echo-cancel

To display the echo-cancellation information of T1/E1 multiflex voice/WAN interface cards, use the **show echo-cancel** command in privileged EXEC mode.

show echo-cancel hardware status *slot-number*

Syntax Description

hardware	Displays information about the hardware accelerated EC device.
status	Displays the allocation status.
slot-number	The slot number of the interface cards.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.4(24)T	This command was introduced in a release earlier than Cisco IOS Release 12.4(24)T.

Usage Guidelines

Hardware echo cancellation is restricted to the same baseboard voice/WAN interface card (VWIC) on which the daughter card (EC-MFT-32 and EC-MFT-64) is installed and cannot be shared by other T1/E1 controllers.

Examples

The following is sample output from the **show echo-cancel hardware status**command:

```
Router# show echo-cancel hardware status
ECAN CH   Assigned   DSP ID   VOICEPORT   EC   NLP   COV  LAW
=============================================================
   0          yes       8       1/0/0      on   off   on   u-Law
   1          no        -          -       off  on    on   u-Law
   2          no        -          -       off  on    on   u-Law
   3          no        -          -       off  on    on   u-Law
   4          no        -          -       off  on    on   u-Law
   5          no        -          -       off  on    on   u-Law
```

The table below describes the significant fields shown in the display.

Table 71: show echo-cancel Field Descriptions

Field	Description
ECAN CH	Total channels in the slot.
Assigned	Status of the assigned channels.
DSP ID	Digital Signaling Processor (DSP) identification number for the assigned channels.
VOICEPORT	Voice port of the channels.
EC	Echo Cancellation status of the assigned channels.

Field	Description
NLP	Status of the Non-Linear Processor (NLP).
COV	Echo cancellation Coverage status of the assigned channels.

show event-manager consumers

To display event-manager statistics for debugging purposes, use the **show event-manager consumers**command in privileged EXEC mode.

show event-manager consumers

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.3(4)T	This command was introduced.

Examples

The following example shows one call (two call legs) going through the gateway:

```
Router# show event-manager consumers
Hash table indexed by AAA_UNIQUE_ID
Uid        Consumer_id  Consumer_hdl  evt_type
00000015   0002         65B35570      START
00000015   0002         65B35570      STOP
00000016   0002         65B34ECC      START
00000016   0002         65B34ECC      STOP
```

The table below lists and describes the significant output fields.

Table 72: show event-manager consumers Field Descriptions

Field	Description
Uid	User ID.
Consumer_id	ID of the consumer client process.
Consumer_hdl	Handler of the consumer client process.
evt_type	Event type.

Related Commands

Command	Description
show voice statistics csr interval accounting	Displays all accounting CSRs specified by interval number.
show voice statistics csr interval aggregation	Displays signaling CSRs specified by interval number.
show voice statistics csr since-reset accounting	Displays all accounting CSRs since the last reset.
show voice statistics csr since-reset aggregation-level	Displays all signaling CSRs since the last reset.

Command	Description
show voice statistics csr since-reset all	Displays all CSRs since the last reset.
show voice statistics interval-tag	Displays the configured interval numbers.
show voice statistics memory-usage	Displays current memory usage.

show frame-relay vofr

To display information about the FRF.11 subchannels being used on Voice over Frame Relay (VoFR) data link connection identifiers (DLCIs), use the **show frame-relay vofr** command in privileged EXEC mode.

show frame-relay vofr [*interface* [*dlci* [*cid*]]]

Syntax Description

interface	(Optional) Specific interface type and number for which you want to display FRF.11 subchannel information.
dlci	(Optional) Specific data link connection identifier for which you want to display FRF.11 subchannel information.
cid	(Optional) Specific subchannel for which you want to display information.

Command Default

If this command is entered without a specified interface, FRF.11 subchannel information is displayed for all VoFR interfaces and DLCIs configured on the router.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.0(4)T	This command was introduced on the Cisco 2600 series, Cisco 3600 series, and Cisco MC3810 series.

Examples

The following is sample output from this command when an interface is not specified:

```
Router# show frame-relay vofr
interface         vofr-type   dlci   cid   cid-type
Serial0/0.1       VoFR        16     4     data
Serial0/0.1       VoFR        16     5     call-control
Serial0/0.1       VoFR        16     10    voice
Serial0/1.1       VoFR cisco  17     4     data
```

The following is sample output from this command when an interface is specified:

```
Router# show frame-relay vofr serial0
interface         vofr-type   dlci   cid   cid-type
Serial0           VoFR        16     4     data
Serial0           VoFR        16     5     call-control
Serial0           VoFR        16     10    voice
```

The following is sample output from this command when an interface and a DLCI are specified:

```
Router# show frame-relay vofr serial0 16
VoFR Configuration for interface Serial0
dlci vofr-type  cid cid-type          input-pkts    output-pkts   dropped-pkts
16   VoFR       4   data              0             0             0
16   VoFR       5   call-control      85982         86099         0
16   VoFR       10  voice             2172293       6370815       0
```

The following is sample output from this command when an interface, a DLCI, and a CID are specified:

```
Router# show frame-relay vofr serial0 16 10
VoFR Configuration for interface Serial0 dlci 16
  vofr-type  VoFR     cid 10      cid-type voice
  input-pkts 2172293   output-pkts 6370815   dropped-pkts 0
```

The table below describes significant fields shown in this output.

Table 73: show frame-relay vofr Field Descriptions

Field	Description
interface	Number of the interface that has been selected for observation of FRF.11 subchannels.
vofr-type	Type of VoFR DLCI being observed.
cid	Portion of the specified DLCI that is carrying the designated traffic type. A DLCI can be subdivided into 255 subchannels.
cid-type	Type of traffic carried on this subchannel.
input-pkts	Number of packets received by this subchannel.
output-pkts	Number of packets sent on this subchannel.
dropped-pkts	Total number of packets discarded by this subchannel.

Related Commands

Command	Description
show call active voice	Displays the contents of the active call table.
show call history voice	Displays the contents of the call history table.
show dial-peer voice	Displays configuration information and call statistics for dial peers.
show frame-relay fragment	Displays Frame Relay fragmentation details.
show frame-relay pvc	Displays statistics about PVCs for Frame Relay interfaces.
show voice-port	Displays configuration information about a specific voice port.

show gatekeeper calls

To display the status of each ongoing call of which a gatekeeper is aware, use the **show gatekeeper calls**command in privilegedEXEC mode.

show gatekeeper calls [**history**]

Syntax Description

history	(Optional) Displays call history information along with internal error codes at the gatekeeper. The number of disconnected calls displayed in response to this command is the *number* specified in the **call-history max-size** *number* command. Use of this **max-size** number helps to reduce CPU usage in the storage and reporting of this information.

Command Default

The default expression of this command displays information for all active calls detected on the gatekeeper.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
11.3(2)NA	This command was introduced.
12.0(3)T	This command was integrated into Cisco IOS Release 12.0(3)T.
12.0(5)T	The output for this command was changed.
12.1(5)XM2	This command was implemented on the Cisco AS5350 and Cisco AS5400.
12.2(4)T	Support for the Cisco AS5300, Cisco AS5350, and Cisco AS5400 is not included in this release.
12.2(2)XB1	This command was implemented on the Cisco AS5850.
12.2(11)T	This command was integrated into Cisco IOS Release 12.2(11)T. This command is supported on the Cisco AS5300, Cisco AS5350, Cisco AS5400, and Cisco AS5850 in this release.
12.4(4)T	The **history** keyword was added to display historical information on disconnected calls.

Usage Guidelines

Use this command to show all active calls currently being handled by a particular Multimedia Conference Manager (MCM) gatekeeper. If you force a disconnect for either a particular call or all calls associated with a particular MCM gatekeeper by using the **clear h323 gatekeeper call** command, the system does not display information about those calls.

Using the **history** keyword displays the number of disconnected calls specified in the **call-history max-size** *number* command. Use of this **max-size**number helps to reduce CPU usage in the storage and reporting of this information.

Examples

The following is sample output showing active calls:

```
Router# show gatekeeper calls
Total number of active calls = 1.
                          GATEKEEPER CALL INFO
```

```
                          ====================
LocalCallID                          Age(secs)    BW
12-3339                              94           768(Kbps)
 Endpt(s):Alias          E.164Addr     CallSignalAddr  Port  RASSignalAddr   Port
   src EP:epA                          10.0.0.0        1720  10.0.0.0        1700
   dst EP:epB@zoneB.com
   src PX:pxA                          10.0.0.0        1720  10.0.0.00       24999
   dst PX:pxB                          255.255.255.0   1720  255.255.255.0   24999
```

The table below describes the significant fields shown in the display.

Table 74: show gatekeeper calls Field Descriptions

Field	Description
LocalCallID	Identification number of the call.
Age(secs)	Age of the call, in seconds.
BW(Kbps)	Bandwidth in use, in kilobytes per second.
Endpt	Role of each endpoint (terminal, gateway, or proxy) in the call (originator, target, or proxy) and the call signaling and Registration, Admission, and Status (RAS) protocol address.
Alias	H.323-Identification (ID) or Email-ID of the endpoint.
E.164Addr	E.164 address of the endpoint.
CallSignalAddr	Call-signaling IP address of the endpoint.
Port	Call-signaling port number of the endpoint.
RASSignalAddr	RAS IP address of the endpoint.
Port	RAS port number of the endpoint.

Related Commands

Command	Description
clear h323 gatekeeper call	Forces the disconnection of a specific call or of all calls active on a particular gatekeeper.
call history max	Specifies the number of records to be kept in the history table.

show gatekeeper circuits

To display the circuit information on a gatekeeper, use the **show gatekeeper circuits** command in privileged EXEC mode.

show gatekeeper circuits [{**begin** | **exclude** | **include**} *expression*]

Syntax Description

begin	(Optional) Displays all circuits, beginning with the line containing the *expression.*
exclude	(Optional) Displays all circuits, excluding those containing the *expression.*
include	(Optional) Displays all circuits, including those containing the *expression.*
expression	(Optional) Word or phrase used to determine what lines are displayed.

Command Default

Shows all circuit information.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(11)T	This command was introduced.

Usage Guidelines

Use this command to display current configuration information about the circuits that are registered with the gatekeeper.

Examples

The following command displays the circuit information for the gatekeeper:

```
Router# show gatekeeper circuits
Circuit       Endpoint   Max Calls Avail Calls Resources     Zone
-------       --------   --------- ----------- ---------     ----
CarrierA      Total Endpoints: 2
              3640-gw1   25        25          Available
              5400-gw1   23        19          Unavailable
CarrierB      Total Zones: 1
                                                           MsPacmanGK
```

The table below describes the fields shown in this output.

Table 75: show gatekeeper circuits Field Descriptions

Field	Description
Circuit	Name of the each circuit connected to the gatekeeper.
Endpoint	Name of each H.323 endpoint.
Max Calls	Maximum number of calls that circuit can handle.
Avail Calls	Number of new calls that the circuit can handle at the current time.

Field	Description
Resources	Whether the circuit's resources have exceeded the defined threshold limits. The **endpoint resource-threshold** command defines these thresholds.
Zone	Zone that supports the endpoint. The **zone circuit-id** command assigns a zone to an endpoint.
Total Endpoints	Total number of endpoints supported by the circuit.
Total Zones	Total number of zones supported by the circuit.

Related Commands

Command	Description
endpoint resource-threshold	Sets a gateway's capacity thresholds in the gatekeeper.
zone circuit-id	Assigns a remote zone to a carrier.

show gatekeeper cluster

To display all the configured gatekeeper clusters information, use the **show gatekeeper cluster** command in user EXEC or privileged EXEC mode.

show gatekeeper cluster

Syntax Description

This command has no arguments or keywords.

Command Modes

User EXEC (>)
Privileged EXEC (#)

Command History

Release1.25	Modification
12.1(5)XM	This command was introduced.
12.2(2)T	This command was integrated into Cisco IOS Release 12.2(2)T.
12.2(2)XB1	This command was integrated into Cisco IOS Release 12.2(2)XB1 and implemented on the Cisco AS5850 router.

Examples

The following is sample output from the **show gatekeeper cluster** command. Field descriptions are self-explanatory.

```
Router# show gatekeeper cluster
                    CONFIGURED CLUSTERS
                    ===================
Cluster Name    Type     Local Zone   Elements  IP
------------    ----     ----------   --------  --
Cluster A       Local    AGK1         AGK2      192.168.200.254 1719
                                      AGK3      192.168.200.223 1719
Cluster B       Remote               BGK1      192.168.200.257 1719
                                      BGK2      192.168.200.258 1719
                                      BGK3      192.168.200.259 1719
```

Related Commands

Command	Description
show gatekeeper endpoints	Displays the status of all registered endpoints for a gatekeeper.
show gatekeeper performance stats	Displays the performance statistics on the the gatekeeper level message.
show gatekeeper zone cluster	Displays the dynamic status of all local clusters.

show gatekeeper endpoint circuits

To display information on all registered endpoints and carriers or trunk groups for a gatekeeper, use the **show gatekeeper endpoint circuits**command in privileged EXEC mode.

show gatekeeper endpoint circuits [{**begin** | **exclude** | **include**} *expression*]

Syntax Description

| begin	(Optional) Displays all circuits, beginning with the line that contains *expression.*
| exclude	(Optional) Displays all circuits, excluding those that contain *expression.*
| include	(Optional) Displays all circuits, including those that contain *expression.*
expression	(Optional) Word or phrase used to determine what lines are displayed.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
11.3(2)NA	This command was introduced.
12.0(5)T	The display format was modified for H.323 Version 2.
12.2(11)T	The display format was modified to show the E.164 ID, carrier and trunk group data, and total number of active calls.

Usage Guidelines

Use this command to display current configuration information about the endpoints and carriers registered with the gatekeeper. Note that you must type the pipe (|) before any of the optional keywords.

Examples

The following command displays the circuit information for the gatekeeper:

```
Router# show gatekeeper endpoint circuits
                    GATEKEEPER ENDPOINT REGISTRATION
                    ================================
CallSignalAddr  Port  RASSignalAddr   Port  Zone Name         Type    Flags
--------------- ----- --------------- ----- ---------         ----    -----
172.18.195.120  1720  172.18.195.120  51059 LavenderGK        VOIP-GW
    E164-ID: 4081234
    H323-ID: 3640-gw1
    Carrier: CarrierA, Max Calls: 25, Available: 25
172.18.197.143  1720  172.18.197.143  57071 LavenderGK        VOIP-GW
    H323-ID: 5400-gw1
    Carrier: CarrierB, Max Calls: 23, Available: 19
    Carrier: CarrierA, Max Calls: 25, Available: 25
Total number of active registrations = 2
```

The table below describes the fields shown in this output.

Table 76: show gatekeeper endpoint circuits Fields

Field	Description
CallsignalAddr	Call signaling IP address of the endpoint. If the endpoint is also registered with an alias, a list of all aliases registered for that endpoint should be listed on the line below.
Port	Call signaling port number of the endpoint.
RASSignalAddr	RAS IP address of the endpoint.
Port	RAS port number of the endpoint.
Zone Name	Zone name (gatekeeper ID) that this endpoint registered in.
Type	Endpoint type (for example, terminal, gateway, or MCU).
Flags	S--Endpoint is statically entered from the **alias**command rather than being dynamically registered through RAS messages. O--Endpoint, which is a gateway, has sent notification that it is nearly out of resources.
E164-ID	E.164 ID of the endpoint.
H323-ID	H.323 ID of the endpoint.
Carrier	Carrier associated with the endpoint.
Max Calls	Maximum number of calls the circuit can handle.
Available	Number of new calls the circuit can handle currently.

Related Commands

Command	Description
endpoint circuit-id h323id	Assigns a circuit to a non-Cisco endpoint.
endpoint resource-threshold	Sets a gateway's capacity thresholds in the gatekeeper.
zone circuit-id	Assigns a circuit to a remote zone.

show gatekeeper endpoints

To display the status of all registered endpoints for a gatekeeper, use the **show gatekeeper endpoints** command in privileged EXEC mode.

show gatekeeper endpoints [**alternates**]

Syntax Description

alternates	(Optional) Displays information about alternate endpoints. All information normally included with this command is also displayed.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
11.3(2)NA	This command was introduced.
12.0(5)T	The display format was modified for H.323 Version 2.
12.1(5)XM	The **alternates** keyword was added.
12.1(5)XM2	This command was implemented on the Cisco AS5350 and Cisco AS5400.
12.2(2)T	This command was integrated into Cisco IOS Release 12.2(2)T.
12.2(4)T	This command was not supported on the Cisco AS5300, Cisco AS5350, and Cisco AS5400 in this release.
12.2(2)XB1	This command was implemented on the Cisco AS5850.
12.2(11)T	This command was integrated into Cisco IOS Release 12.2(11)T. The registration and call capacity values were added to the output display.
12.3(1)	This command was modified to reflect concurrent calls for the endpoints.

Examples

The following is sample output from this command:

```
Router# show gatekeeper endpoints
CallsignalAddr   Port  RASSignalAddr   Port   Zone Name    Type     F
---------------  ----  -------------   -----  ----------   -----    --
172.21.127.8     1720  172.21.127.8    24999  sj-gk        MCU
H323-ID:joe@cisco.com
           Voice Capacity Max.=23  Avail.=23
           Total number of active registrations = 1
172.21.13.88     1720  172.21.13.88    1719   sj-gk        VOIP-GW   O    H323-ID:la-gw
```

The table below describes significant fields shown in this output.

Table 77: show gatekeeper endpoints Field Descriptions

Field	Description
CallsignalAddr	Call signaling IP address of the endpoint. If the endpoint is also registered with an alias (or aliases), a list of all aliases registered for that endpoint should be listed on the line below.
Port	Call signaling port number of the endpoint.
RASSignalAddr	Registration, Admission, and Status (RAS) protocol IP address of the endpoint.
Port	RAS port number of the endpoint.
Zone Name	Zone name (gatekeeper identification [ID]) to which this endpoint is registered.
Type	Endpoint type (for example, terminal, gateway, or multipoint control unit [MCU]).
F	S--Endpoint is statically entered from the **alias** command rather than being dynamically registered through RAS messages. O--Endpoint, which is a gateway, has sent notification that it is nearly out of resources.
Voice Capacity Max.	Maximum number of channels available on the endpoint.
Avail.	Current number of channels available on the endpoint.
Total number of active registrations	Total number of endpoints registered with the gatekeeper.

In the following example, the **show gatekeeper endpoints** output has been modified to reflect concurrent calls for the endpoint. If an endpoint is not reporting capacity and the **endpoint max-calls h323id** command is not configured, "Voice Capacity Max." and "Avail." will not be shown. "Current.= 2" indicates that the current active calls for the endpoint are 2.

```
Router# show gatekeeper endpoints
!
                    GATEKEEPER ENDPOINT REGISTRATION
                    ================================
CallSignalAddr  Port  RASSignalAddr   Port  Zone Name         Type    Flags
--------------- ----  -------------   ----  ---------         ----    -----
172.18.200.27   1720  172.18.200.27   49918 GK-1              VOIP-GW
    H323-ID:GW1
    Voice Capacity Max.=  Avail.=  Current.= 2
```

If an endpoint is reporting capacity but the **endpoint max-calls h323id** command is not configured, "Voice Capacity Max." and "Avail." will show reported call capacity of the endpoint as follows:

```
Router# show gatekeeper endpoints
!
                    GATEKEEPER ENDPOINT REGISTRATION
                    ================================
CallSignalAddr  Port  RASSignalAddr  Port  Zone Name          Type  Flags
--------------  ----  -------------  ----  ---------          ----  -----
```

```
172.18.200.29   1720  172.18.200.29  53152 GK-2              VOIP-GW
    H323-ID:GW2
    Voice Capacity Max.= 23 Avail.= 22 Current.= 1
```

If an endpoint is reporting capacity but the **endpoint max-calls h323id** command is not configured, "Voice Capacity Max." will show the maximum calls configured and "Avail." will show the available calls of the endpoint. In this example, "Voice Capacity Max.= 10" is showing that the maximum calls configured for the endpoint are 10. "Avail.= 2" shows that currently available calls for the endpoint are 2. "Current.= 8" shows that current active calls for the endpoint are 8.

```
Router# show gatekeeper endpoints
!
                    GATEKEEPER ENDPOINT REGISTRATION
                    ================================
CallSignalAddr  Port  RASSignalAddr   Port  Zone Name         Type     Flags
--------------  ----  -------------   ----  ---------         ----     -----
172.18.200.27   1720  172.18.200.27   49918 GK-1              VOIP-GW
    H323-ID:GW1
    Voice Capacity Max.= 10  Avail.= 2  Current.= 8
```

The table below describes significant fields in the output examples.

Table 78: show gatekeeper endpoints Field Descriptions

Field	Description
CallsignalAddr	Call signaling IP address of the endpoint. If the endpoint is also registered with an alias (or aliases), a list of all aliases registered for that endpoint should be listed on the line below.
Port	Call signaling port number of the endpoint.
RASSignalAddr	Registration, Admission, and Status (RAS) protocol IP address of the endpoint.
Port	RAS port number of the endpoint.
Zone Name	Zone name (gatekeeper ID) to which this endpoint is registered.
Type	The endpoint type (for example, terminal, gateway, or multipoint control unit [MCU]).
Flags	S--Endpoint is statically entered from the **alias** command rather than being dynamically registered through RAS messages. O--Endpoint, which is a gateway, has sent notification that it is nearly out of resources.

Related Commands

Command	Description
endpoint resource-threshold	Sets a gateway's capacity thresholds in the gatekeeper.
show gatekeeper endpoint circuits	Displays endpoint and carrier or trunk group call capacities.
show gatekeeper gw-type-prefix	Displays the gateway technology prefix table.
show gatekeeper zone status	Displays the status of zones related to a gatekeeper.
show gateway	Displays the current gateway status.

show gatekeeper gw-type-prefix

To display the gateway technology prefix table, use the **show gatekeeper gw-type-prefix** command in privileged EXEC mode.

show gatekeeper gw-type-prefix

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
11.3(2)NA	This command was introduced.
12.0(5)T	The display format was modified for H.323 Version 2.
12.1(5)XM2	This command was implemented on the Cisco AS5350 and Cisco AS5400.
12.2(4)T	This command was not supported on the Cisco AS5300, Cisco AS5350, and Cisco AS5400 in this release.
12.2(2)XB1	This command was implemented on the Cisco AS5850.
12.2(11)T	This command was integrated into Cisco IOS Release 12.2(11)T.

Examples

The following is sample output from this command for a gatekeeper that controls two local zones, sj-gk and la-gk:

```
Router# show gatekeeper gw-type-prefix
GATEWAY TYPE PREFIX TABLE
=========================
Prefix:12#*     (Default gateway-technology)
  Zone sj-gk master gateway list:
    10.0.0.0:1720 sj-gw1
    10.0.0.0:1720 sj-gw2 (out-of-resources)
    10.0.0.0:1720 sj-gw3
  Zone sj-gk prefix 408....... priority gateway list(s):
   Priority 10:
    10.0.0.0:1720 sj-gw1
   Priority 5:
    10.0.0.0:1720 sj-gw2 (out-of-resources)
    10.0.0.0:1720 sj-gw3
Prefix:7#*     (Hopoff zone la-gk)
  Statically-configured gateways (not necessarily currently registered):
    10.0.0.0:1720
    10.0.0.0:1720
  Zone la-gk master gateway list:
    10.0.0.0:1720 la-gw1
    10.0.0.0:1720 la-gw2
```

The table below describes significant fields shown in this output.

Table 79: show gatekeeper gw-type-prefix Field Descriptions

Field	Description
Prefix	Technology prefix defined with the **gw-type-prefix** command.
Zone sj-gk master gateway list	List of all the gateways registered to zone sj-gk with the technology prefix under which they are listed. (This display shows that gateways sj-gw1, sj-gw2, and sj-gw3 have registered in zone sj-gk with the technology prefix 12#.)
Zone sj-gk prefix 408..... priority gateway list(s)	List of prioritized gateways to handle calls to area code 408.
Priority 10	Highest priority level. Gateways listed following "Priority 10" are given the highest priority when selecting a gateway to service calls to the specified area code. (In this display, gateway sj-gw1 is given the highest priority to handle calls to the 408 area code.)
Priority 5	Any gateway that does not have a priority level assigned to it defaults to priority 5.
(out-of-resources)	Indication that the displayed gateway has sent a "low-in-resources" notification.
(Hopoff zone la-gk)	Any call that specifies this technology prefix should be directed to hop off in the la-gk zone, no matter what the area code of the called number is. (In this display, calls that specify technology prefix 7# are always routed to zone la-gk, regardless of the actual zone prefix in the destination address.)
Zone la-gk master gateway list	List of all the gateways registered to la-gk with the technology prefix under which they are listed. (This display shows that gateways la-gw1 and la-gw2 have registered in zone la-gk with the technology prefix 7#. No priority lists are displayed here because none were defined for zone la-gk.)
(Default gateway-technology)	If no gateway-type prefix is specified in a called number, then gateways that register with 12# are the default type to be used for the call.
Statically-configured gateways	List of all IP addresses and port numbers of gateways that are incapable of supplying technology-prefix information when they register. This display shows that, when gateways 1.1.1.1:1720 and 2.2.2.2:1720 register, they are considered to be of type 7#.

Related Commands

Command	Description
show gatekeeper calls	Displays the status of each ongoing call of which a gatekeeper is aware.
show gatekeeper endpoints	Displays the status of all registered endpoints for a gatekeeper.
show gateway	Displays the current gateway status.

show gatekeeper performance statistics

To display performance statistics on the gatekeeper level message, use the **show gatekeeper performance stats** command in user EXEC or privileged EXEC mode.

show gatekeeper performance statistics [**zone** [**name** *zone-name*]] [**cumulative**]

Syntax Description

zone	(Optional) Displays zone statistics of the gatekeeper.
name *zone -name*	(Optional) Specifies the zone name or gatekeeper name.
cumulative	(Optional) Displays the total statistics collected by the gatekeeper since the last reload.

Command Modes

User EXEC (>)
Privileged EXEC (#)

Command History

Release	Modification
12.1(5)XM	This command was introduced.
12.2(2)T1	This command was integrated into Cisco IOS Release 12.2(2)T.
12.2(2)XB1	This command was implemented on the Cisco AS5850.
12.2(15)T	This command was modified. The **zone**, **name**, and **cumulative** keywords were added and the *zone-name* argument was added.
12.4(5)	This command was modified. Command output was enhanced to include counters for: • Automatic rejections (ARJs) sent due to an ARQ access-list denial. • Location rejections (LRJs) sent due to an LRQ access-list denial.

Usage Guidelines

Use this command to display the statistics on calls, registration, calls routed to other gatekeepers, and calls used via zone processing.

When the **cumulative** keyword is used along with **zone name** keywords displays the total statistics for the specified zone, from the starting time of the gatekeeper. These values are not reset when the **clear h323 gatekeeper stats**command is used.

This command displays statistical data related to the router. You can identify the number of call initiation events using the following messages:

- Automatic repeat request (ARQ)
- Admission confirmation (ACF)
- Admission rejection (ARJ)

You can identify endpoint contact events that have been requested and either confirmed or rejected on the router using the following:

- Location request (LRQ)
- Location confirm (LCF)
- Location reject (LRJ)

The counts associated with overload and the number of endpoints sent to alternate gatekeepers that are associated with overload conditions are also displayed. Only when the router experiences an overload condition do these counters reveal a value other than zero. The real endpoint count simply displays the number of endpoints registered on this router platform. The time stamp displays the start time when the counters started capturing the data. When you want to request a new start period, enter the **clear h323 gatekeeper stats** command. The counters are reset and the time stamp is updated with the new time.

You can identify remote gatekeeper contacts that have been requested and either confirmed or rejected on the router using the following messages:

- Location confirm (LCF)
- Location rejection (LRJ)
- Location request (LRQ)

You can identify zone-level or gatekeeper-level registration statistics using the following messages:

- Registration confirmation (RCF)
- Registration rejection (RRJ)
- Registration request (RRQ)

You can identify zone-level or gatekeeper-level unregistration statistics using the following messages:

- Unregistration confirmation (UCF)
- Unregistration rejection (URJ)
- Unregistration request (URQ)

Examples

The following is the example of basic output from the **show gatekeeper performance stats** command. The basic output specifies that the counters are reset using the **clear h323 gatekeeper stats** command and the output displays the statistcs from the last reset.

```
Router# show gatekeeper performance stats
-----Gatekeeper Performance Statistics-----
Performance statistics captured since: 20:09:00 UTC Thu Sep 15 2005
Gatekeeper level Admission Statistics:
        ARQs received: 1
        ARQs received from originating endpoints: 0
        ACFs sent: 1
        ACFs sent to the originating endpoint: 0
        ARJs sent: 0
        ARJs sent to the originating endpoint: 0
        ARJs sent due to overload: 0
        ARJs sent due to ARQ access-list denial: 0
        Number of concurrent calls: 0
        Number of concurrent originating calls: 0
Gatekeeper level Location Statistics:
        LRQs received: 3
```

```
        LRQs sent: 0
        LCFs received: 0
        LCFs sent: 1
        LRJs received: 0
        LRJs sent: 2
        LRJs sent due to overload: 0
        LRJs sent due to LRQ access-list denial: 2
Gatekeeper level Registration Statistics:
        RRJ due to overload: 0
        Total Registered  Endpoints: 2
Gatekeeper level Disengage Statistics:
        DRQs received: 1
        DRQs sent: 0
        DCFs received: 0
        DCFs sent: 1
        DRJs received: 0
        DRJs sent: 0
Gatekeeper viazone message counters:
        inARQ: 0
        infwdARQ: 0
        inerrARQ: 0
        inLRQ: 0
        infwdLRQ: 0
        inerrLRQ: 0
        outLRQ: 0
        outfwdLRQ: 0
        outerrLRQ: 0
        outARQ: 0
        outfwdARQ: 0
        outerrARQ: 0
Load balancing events: 0
```

The following is the example of cumulative output from the **show gatekeeper performance stats** command. The cumulative output specifies that the counters are not reset and the output displays the total statistcs from the starting time of the gatekeeper.

```
Router# show gatekeeper performance stats zone name voip3-2600-2
Performance statistics for zone voip3-2600-2
-----Zone Level Performance Statistics-----
Performance statistics captured since: 00:17:00 UTC Mon Mar 1 1993
Zone level Admission Statistics:
        ARQs received: 1
        ARQs received from originating endpoints: 0
        ACFs sent: 1
        ACFs sent to the originating endpoint: 0
        ARJs sent: 0
        ARJs sent to the originating endpoint: 0
        Number of concurrent total calls: 0
        Number of concurrent originating calls: 0
Zone level Location Statistics:
        LRQs received: 1
        LRQs sent: 0
        LCFs received: 0
        LCFs sent: 1
        LRJs received: 0
        LRJs sent: 0
Zone level Registration Statistics:
        Full RRQs received: 1
        Light RRQs received: 574
        RCFs sent: 576
        RRJs sent: 0
        Total Registered Endpoints: 1
Zone level UnRegistration Statistics:
```

```
        URQs received: 0
        URQs sent: 0
        UCFs received: 0
        UCFs sent: 0
        URJs received: 0
        URJs sent: 0
        URQs sent due to timeout: 0
Zone level Disengage Statistics:
        DRQs received: 1
        DRQs sent: 0
        DCFs received: 0
        DCFs sent: 1
        DRJs received: 0
        DRJs sent: 0
```

The table below shows significant fields shown in the displays. Most of the fields are self-explanatory and are not listed the table.

Table 80: show gatekeeper performance statistics Field Descriptions

Field	Description
Full RRQs received	A full registration request (RRQ) contains all registration information that is used for successful registration.
Light RRQs received	A light RRQ contains abbreviated registration information that is used to maintain an existing registration.

Related Commands

Command	Description
clear h323 gatekeeper stats	Clears statistics about gatekeeper performance.

show gatekeeper servers

To display a list of currently registered and statically configured triggers on a gatekeeper router, use the **show gatekeeper servers** command in EXEC mode.

show gatekeeper servers [*gkid*]

Syntax Description

gkid	(Optional) Local gatekeeper name to which this trigger applies.

Command Modes

EXEC (#)

Command History

Release	Modification
12.1(1)T	This command was introduced on the Cisco 2500 series, Cisco 2600 series, Cisco 3600 series, Cisco 7200, and Cisco MC3810.
12.2(2)XB	The output of this command was modified to show additional server statistics, including the following: gatekeeper server timeout value; Gatekeeper Transaction Message Protocol (GKTMP) version installed; number of Registration Request (RRQ), Registration Response (RRQ), Response Confirmation (RCF), and Response Reject (RRJ) messages received; timeouts encountered; average response time; and if the server is usable.
12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T.
12.2(11)T	This command was implemented on the Cisco 3700 series.
12.2(15)T12	The command was modified to show additional server statistics.
12.3(8)T	The command was modified to show additional server statistics.
12.3(9)	The command was modified to show additional server statistics.

Usage Guidelines

Use this command to show all server triggers (whether dynamically registered from the external servers or statically configured from the command-line interface) on this gatekeeper. If the gatekeeper ID is specified, only triggers applied to the specified gatekeeper zone appear. If the gatekeeper ID is not specified, server triggers for all local zones on this gatekeeper appear.

Examples

The following is sample output from this command:

```
Router# show gatekeeper servers
            GATEKEEPER SERVERS STATUS
            =========================
Gatekeeper Server listening port: 8250
Gatekeeper Server timeout value: 30 (100ms)
GateKeeper GKTMP version: 4.1
Gatekeeper-ID: Gatekeeper1
------------------------
RRQ Priority: 5
Server-ID: Server43
Server IP address: 209.165.200.254:40118
```

```
Server type: dynamically registered
Connection Status: active
Trigger Information:
Trigger unconditionally
Server Statistics:
REQUEST RRQ Sent=0
RESPONSE RRQ Received = 0
RESPONSE RCF Received = 0
RESPONSE RRJ Received = 0
Average response time(ms)=0
Server Usable=TRUE
Timeout Statistics:
Server-ID: Server43
Server IP address: 209.165.200.254:40118
Server type: dynamically registered
Connection Status: active
Timeout Encountered=0
```

The table below describes significant fields shown in this output.

Table 81: show gatekeeper servers Field Descriptions

Field	Description
GateKeeper GKTMP version	Version of Gatekeeper Transaction Message Protocol installed.
RRQ Priority	Registration priority.
Server-ID	Server ID name.
Server IP address	Server IP address.
Server type	Type of server.
Connection Status	Whether the connection is active or inactive.
Trigger Information	Which Registration, Admission, and Status (RAS) messages the Cisco IOS gatekeeper forwards to the external application.
REQUEST RRQ	Registration requests received.
RESPONSE RRQ	Registration responses received.
RESPONSE RCF	Response confirmations received.
RESPONSE RRJ	Response reject messages received.

Related Commands

Command	Description
debug gatekeeper server	Traces all the message exchanges between the Cisco IOS gatekeeper and the external applications.
endpoint circuit-id h323id	Tracks call capacity information on the gatekeeper.
server registration-port	Configures a listening port on the gatekeeper for server registration.
server trigger arq	Configures static triggers on the gatekeeper.

show gatekeeper status

To display overall gatekeeper status, including authorization and authentication status and zone status, use the **show gatekeeper status**command in privileged EXEC mode.

show gatekeeper status

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
11.3(2)NA	This command was introduced.
12.0(3)T	This command was integrated into Cisco IOS Release 12.0(3)T.
12.1(5)XM	This command was modified to show information about load balancing and vendor-specific attributes.
12.2(2)T	This command was integrated into Cisco IOS Release 12.2(2)T.
12.2(2)XB	This command was modified to show information about server flow control.
12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T.

Examples

The following is sample output from this command:

```
Router# show gatekeeper status
Gatekeeper State: UP
    Load Balancing:   DISABLED
    Flow Control:     ENABLED
    Zone Name:        snet-3660-3
    Accounting:       DISABLED
    Endpoint Throttling:        DISABLED
    Security:         DISABLED
    Maximum Remote Bandwidth:              unlimited
    Current Remote Bandwidth:              0 kbps
    Current Remote Bandwidth (w/ Alt GKs): 0 kbps
```

The table below describes significant fields shown in this output.

Table 82: show gatekeeper status Field Descriptions

Field	Description
Gatekeeper State	Gatekeeper state has the following values: • UP is operational. • DOWN is administratively shut down. • INACTIVE is administratively enabled; that is, the **no shutdown** command has been issued, but no local zones have been configured. • HSRP STANDBY indicates that the gatekeeper is on hot standby and will take over when the currently active gatekeeper fails.
Load Balancing	Whether load balancing is enabled.
Flow Control	Whether server flow control is enabled.
Zone Name	Zone name to which the gatekeeper belongs.
Accounting	Whether authorization and accounting features are enabled.
Endpoint Throttling	Whether endpoint throttling is enabled.
Security	Whether security features are enabled.
Bandwidth	Maximum remote bandwidth, current remote bandwidth, and current remote bandwidth with alternate gatekeepers.

Related Commands

Command	Description
show gatekeeper servers	Displays statistics about the gatekeeper.

show gatekeeper status cluster

To display information about each element of a local cluster, such as the amount of memory used, the number of active calls, and the number of endpoints registered on the element, use the **show gatekeeper status cluster** command in privileged EXEC mode.

show gatekeeper status cluster

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.1(5)XM1	This command was introduced.
12.2(2)T	This command was integrated into Cisco IOS Release 12.2(2)T.
12.2(2)XB1	This command was implemented on the Cisco AS5850.

Examples

The following command displays information about elements of a local cluster, two of whose components are RoseGK and LavenderGK:

```
Router# show gatekeeper status cluster
                   CLUSTER INFORMATION
                   ==================
                                  Active     Endpoint       Last
Hostname      %Mem    %CPU     Calls        Count   Announce
--------      ----    ----    ------     --------   --------
RoseGK          72       0         1   Local Host
LavenderGK      30       1         0            4        14s
```

Related Commands

Command	Description
show gatekeeper endpoints	Displays the status of all registered endpoints for a gatekeeper.
show gatekeeper performance statistics	Displays information about the number of calls accepted and rejected, and finds the number of endpoints sent to other gatekeepers.
show gatekeeper zone cluster	Displays the dynamic status of all local clusters.

show gatekeeper zone cluster

To display the dynamic status of all local clusters, use the **show gatekeeper zone cluster**command in privilegedEXEC mode.

show gatekeeper zone cluster

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.1(5)XM1	This command was introduced.
12.2(2)T	This command was integrated into Cisco IOS Release 12.2(2)T.
12.2(2)XB1	This command was implemented on the Cisco AS5850.

Examples

The following command displays information about the current bandwidth values and about when the last announcement message from the alternate gatekeeper was received. In the following example, PRI represents the priority value assigned to an alternate gatekeeper. This field ranges from 0 to 127, with 127 representing the lowest priority.

```
Router# show gatekeeper zone cluster
                 LOCAL CLUSTER INFORMATION, 6t
                 ============================
                                        TOT BW   INT BW   REM BW   LAST       ALT GK
LOCAL GK NAME    ALT GK NAME    PRI    (kbps)   (kbps)   (kbps)   ANNOUNCE   STATUS
-------------    -----------    ---    ------   ------   ------   --------   ------
ParisGK          GenevaGK       120    0        0        0        7s         CONNECTED
NiceGK           ZurichGK       100    0        0        0        7s         CONNECTED
```

Related Commands

Command	Description
timer cluster -element announce	Defines the time interval between successive announcement messages exchanged between elements of a local cluster.
zone cluster local	Defines a local grouping of gatekeepers.
zone remote	Statically specifies a remote zone if DNS is unavailable or undesirable.

show gatekeeper zone prefix

To display the zone prefix table, use the **show gatekeeper zone prefix**command in privileged EXEC mode.

show gatekeeper zone prefix [**all**]

Syntax Description

all	(Optional) Displays the dynamic zone prefixes registered by each gateway.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
11.3(2)NA	This command was introduced.
12.2(15)T	The **all** keyword was added.

Usage Guidelines

If the **all** keyword is not specified, this command displays the static zone prefixes only. Use the **include** filter with the **all** keyword to display the prefixes associated with a particular gateway. For example, the **show gatekeeper zone prefix all | include GW1** command displays the dynamic prefixes associated with gateway GW1.

Examples

The following command displays the zone prefix table for the gatekeeper:

```
Router# show gatekeeper zone prefix
      ZONE PREFIX TABLE
      =================
GK-NAME               E164-PREFIX
-------               -----------
gk2                   408*
gk2                   5551001*
gk2                   5551002*
gk2                   5553020*
gk2                   5553020*
gk1                   555....
gk2                   719*
gk2                   919*
```

The following command displays the zone prefix table, including the dynamic zone prefixes, for the gatekeeper:

```
Router# show gatekeeper zone prefix all
                    ZONE PREFIX TABLE
      ================================================
GK-NAME               E164-PREFIX       Dynamic GW-priority
-------               -----------       -------------------
gk2                   408*
gk2                   5551001*            GW1 /5
gk2                   5551002*            GW1 /5 GW2 /10
gk2                   5553020*            GW1 /8
gk2                   5553020*
gk1                   555....
```

```
gk2                  719*
gk2                  919*                GW2 /5
```

The table below describes significant fields shown in this output.

Table 83: show gatekeeper zone prefix Field Descriptions

Field	Description
GK-NAME	Gatekeeper name.
E164-PREFIX	E.164 prefix and a dot that acts as a wildcard for matching each remaining number in the telephone number.
Dynamic GW-priority	Gateway that serves this E164 prefix. Gateway priority. A 0 value prevents the gatekeeper from using the gateway for that prefix. Value 10 places the highest priority on the gateway. The default priority value for a dynamic gateway is 5.

Related Commands

Command	Description
show gatekeeper zone cluster	Displays the dynamic status of all local clusters.

show gatekeeper zone status

To display the status of zones related to a gatekeeper, use the **show gatekeeper zone status** command in privileged EXEC mode.

show gatekeeper zone status

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
11.3(2)NA	This command was introduced.
12.0(5)T	The display format was modified for H.323 Version 2.
12.1(5)XM2	This command was implemented on the Cisco AS5350 and Cisco AS5400.
12.2(4)T	This command was not supported on the Cisco AS5300, Cisco AS5350, and Cisco AS5400 in this release.
12.2(2)XB1	This command was implemented on the Cisco AS5850.
12.2(11)T	This command was integrated into Cisco IOS Release 12.2(11)T.

Examples

The following is sample output from thiscommand:

```
Router# show gatekeeper zone status
                     GATEKEEPER ZONES
                     ================
GK name      Domain Name   RAS Address     PORT  FLAGS MAX-BW   CUR-BW
                                                     (kbps)    (kbps)
-------      -----------   -----------     ----  ----- ------   ------
sj.xyz.com   xyz.com       10.0.0.0        1719  LS             0
  SUBNET ATTRIBUTES :
    All Other Subnets :(Enabled)
  PROXY USAGE CONFIGURATION :
    inbound Calls from germany.xyz.com :
      to terminals in local zone sj.xyz.com :use proxy
      to gateways in local zone sj.xyz.com  :do not use proxy
    Outbound Calls to germany.xyz.com
      from terminals in local zone germany.xyz.com :use proxy
      from gateways in local zone germany.xyz.com  :do not use proxy
    Inbound Calls from all other zones :
      to terminals in local zone sj.xyz.com :use proxy
      to gateways in local zone sj.xyz.com  :do not use proxy
    Outbound Calls to all other zones :
      from terminals in local zone sj.xyz.com :do not use proxy
      from gateways in local zone sj.xyz.com  :do not use proxy
tokyo.xyz.co xyz.com         10.0.0.0        1719  RS             0
milan.xyz.co xyz.com         10.0.0.0        1719  RS             0
```

The table below describes significant fields shown in this output.

Table 84: show gatekeeper zone status Field Descriptions

Field	Description
GK name	Gatekeeper name (also known as the zone name), which is truncated after 12 characters in the display.
Domain Name	Domain with which the gatekeeper is associated.
RAS Address	Registration, Admission, and Status (RAS) protocol address of the gatekeeper.
FLAGS	Displays the following information: • S = static (CLI-configured, not DNS-discovered) • L = local • R = remote
MAX-BW	Maximum bandwidth for the zone, in kbps.
CUR-BW	Current bandwidth in use, in kbps.
SUBNET ATTRIBUTES	List of subnets controlled by the local gatekeeper.
PROXY USAGE CONFIGURATION	Inbound and outbound proxy policies as configured for the local gatekeeper (or zone).

Related Commands

Command	Description
show gatekeeper calls	Displays the status of each ongoing call of which a gatekeeper is aware.
show gatekeeper endpoints	Displays the status of registered endpoints for a gatekeeper.
show gateway	Displays the current gateway status.



show gateway through show modem relay statistics

- show gateway, on page 484
- show h323 calls preserved, on page 486
- show h323 gateway, on page 488
- show h323 gateway prefixes, on page 494
- show http client cache, on page 496
- show http client cache, on page 500
- show http client cookie, on page 503
- show http client history, on page 504
- show http client secure status, on page 505
- show http client statistics, on page 507
- show interface dspfarm, on page 510
- show interfaces cable-modem, on page 515
- show ip address trusted check, on page 519
- show iua as, on page 520
- show iua asp, on page 523
- show media-proxy sessions, on page 525
- show media resource status, on page 529
- show mediacard, on page 530
- show mgcp, on page 533
- show mgcp connection, on page 542
- show mgcp endpoint, on page 546
- show mgcp nas, on page 549
- show mgcp profile, on page 553
- show mgcp srtp, on page 557
- show mgcp statistics, on page 560
- show modem relay statistics, on page 564

show gateway

To display the current status of the gateway, use the **show gateway** command in privileged EXEC mode.

show gateway

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
11.3(6)NA2	This command was introduced.
12.0(5)T	The display format was modified for H.323 Version 2.
12.1(5)XM2	This command was implemented on the Cisco AS5350 and Cisco AS5400.
12.2(4)T	This command was not supported on the Cisco AS5300, Cisco AS5350, and Cisco AS5400 in this release.
12.2(2)XB1	This command was implemented on the Cisco AS5850.
12.2(11)T	This command was integrated into Cisco IOS Release 12.2(11)T.

Examples

The following sample output shows the report that appears when the gateway is not registered with a gatekeeper:

```
Router# show gateway
Gateway gateway1 is not registered to any gatekeeper
Gateway alias list
H323-ID gateway1
H323 resource thresholding is Enabled but NOT Active
H323 resource threshold values:
DSP: Low threshold 60, High threshold 70
DS0: Low threshold 60, High threshold 70
```

This following sample output indicates that an E.164 address has been assigned to the gateway:

```
Router# show gateway
Gateway  gateway1 is registered to Gatekeeper gk1
Gateway alias list
E.164 Number 5551212
H323-ID gateway1
```

The following sample output shows the report that appears when the gateway is registered with a gatekeeper and H.323 resource threshold reporting is enabled with the **resource threshold** command:

```
Router# show gateway
Gateway gateway1 is registered to Gatekeeper gk1
Gateway alias list
H323-ID gateway1
```

```
H323 resource thresholding is Enabled and Active
H323 resource threshold values:
DSP: Low threshold 60, High threshold 70
DS0: Low threshold 60, High threshold 70
```

The following sample output shows the report that appears when the gateway is registered with a gatekeeper and H.323 resource threshold reporting is disabled with the **no resource threshold** command:

```
Router# show gateway
Gateway gateway1 is registered to Gatekeeper gk1
Gateway alias list
H323-ID gateway1
H323 resource thresholding is Disabled
```

Field descriptions should be self-explanatory.

Related Commands

Command	Description
resource threshold	Configures a gateway to report H.323 resource availability to the gatekeeper of the gateway.

show h323 calls preserved

To display data about active H.323 VoIP preserved calls, use the **show h323 calls preserved** command in user EXEC or privileged EXEC mode.

show h323 calls preserved

Command Modes

User EXEC (>)
Privileged EXEC (#)

Command History

Release	Modification
12.4(4)XC	This command was introduced.
12.4(9)T	This command was integrated into Cisco IOS Release 12.4(9)T.

Usage Guidelines

The **show h323 calls preserved** command displays data per preserved call. Only active calls are displayed; preserved call history is not.

If translation rules are configured, the value displayed in the "Calling Number" field may have been translated by a gateway. Gateways handle called number values as the numbers to which calls are routed.

The "CallID" field displays the shorter form of the 16-octet, globally-unique connection ID that is allocated for each call leg. The show call active voice brief command also displays a shorter form of the CallID value (part of the third octet and the fourth octet). The longer form of the CallID value is output by the **show call active voice** command.

The CallID value can be used to refer to a call leg associated with the CallID when issuing other voice commands on the gateway, such as the **show voice call status** command and the **clear call voice** command.

An output value of -1 displayed in the "H225 FD" or "H245 FD" field denotes that the call was preserved due to an error detected on the H.225.0 connection. The actual H.225.0 socket file descriptor used for this call can be found from the syslog message that was output when this call was preserved.

To obtain more information about a call, you can also use the **show call active voice** command. Calls can be cleared with the **clear call voice causecode** command.

Examples

The following is sample output from the **show h323 calls preserved** command where one active call is preserved:

```
Router# show h323 calls preserved
CallID = 11EC , Calling Number = , Called Number = 3210000 ,
RemoteSignallingIPAddress=9.13.0.26 , RemoteSignallingPort=49760 ,
RemoteMediaIPAddress=9.13.0.11 , RemoteMediaPort=17910 , Preserved Duration = 262 , Total
Duration = 562 , H225 FD = -1 , H245 FD = -1
```

The table below provides an alphabetical listing of the fields displayed in the output of the **show h323 calls preserved** command and a description of each field.

Table 85: show h323 calls preserved Field Descriptions

Field	Description
Called Number	The phone number entered by the caller.
CallID	The shortened name for connection ID displayed in the **show call active voice brief** command.
H225 FD	The file descriptor number of the H.225.0 TCP socket.
H245 FD	The file descriptor number of the H.245 TCP socket.
Preserved Duration	The time in seconds that the call has been preserved.
RemoteMediaIPAddress	The remote media IP address.
RemoteMediaPort	The remote media IP address.
RemoteSignallingIPAddress	The remote signaling IP address.
RemoteSignallingPort	The remote signaling port.
Total Duration	The time in seconds of the phone call.

Related Commands

Command	Description
call preserve	Enables the preservation of H.323 VoIP calls.
clear call voice	Clears one or more voice calls detected as inactive because there is no RTP or RTCP activity.
show call active voice	Displays call information for voice calls in progress.
show voice call	Displays the call status for voice ports on the Cisco router.

show h323 gateway

To display statistics for H.323 gateway messages that have been sent and received and to display the reasons for which H.323 calls have been disconnected, use the **show h323 gateway** command in privileged EXEC mode.

show h323 gateway [**cause-code stats** | **h225** | **ras**]

Syntax Description

cause -code stats	(Optional) Output displays the disconnect cause codes that the H.323 subsystem has received. A disconnect can originate either from the far-end gateway or from the opposite call leg on the local gateway.
h225	(Optional) Output lists cumulative counts of the number of H.225 messages that have been sent and received since the counters were last cleared.
ras	(Optional) Output lists the counters for Registration, Admission, and Status (RAS) messages that have been sent to and received from the gatekeeper since the counters were last cleared.

Command Default

To display statistics for all the options, use this command without any of the optional keywords.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.2(4)T	This command was introduced on Cisco H.323 platforms except for the Cisco AS5300, Cisco AS5350, Cisco AS5400, and Cisco AS5850.

Examples

In the following example from a Cisco 3640 router, this command is used without keywords to display the statistics for all the options. See the tables below for descriptions of the fields.

```
Router# show h323 gateway
H.323 STATISTICS AT 01:45:55
H.225 REQUESTS     SENT    RECEIVED    FAILED
Setup              0       5477        0
Setup confirm      5424    0           0
Alert              2734    0           0
Progress           2701    0           0
Call proceeding    5477    0           0
Notify             0       0           0
Info               0       0           0
User Info          0       0           0
Facility           2732    0           0
Release            5198    5313        241
Reject             0       0           0
Passthrough        0       0           0
H225 establish timeout 0
RAS failed            0
H245 failed           0
RAS MESSAGE      REQUESTS SENT    CONFIRMS RCVD    REJECTS RCVD
GK Discovery     grq 0            gcf 0            grj 0
```

```
Registration     rrq 130          rcf 130          rrj 0
Admission        arq 5477         acf 5477         arj 0
Bandwidth        brq 0            bcf 0            brj 0
Disengage        drq 5439         dcf 5439         drj 0
Unregister       urq 0            ucf 0            urj 0
Resource Avail   rai 0            rac 0
Req In Progress  rip 0
RAS MESSAGE      REQUESTS RCVD    CONFIRMS SENT    REJECTS SENT
GK Discovery     grq 0            gcf 0            grj 0
Registration     rrq 0            rcf 0            rrj 0
Admission        arq 0            acf 0            arj 0
Bandwidth        brq 0            bcf 0            brj 0
Disengage        drq 0            dcf 0            drj 0
Unregister       urq 0            ucf 0            urj 0
Resource Avail   rai 0            rac 0
Req In Progress  rip 0
DISC CAUSE CODE           FROM OTHER PEER    FROM H323 PEER
16 normal call clearing   66                 5325
31 normal, unspecified    1                  0
34 no circuit             31                 0
41 temporary failure      3                  0
44 no requested circuit   13                 0
```

In the following example from a Cisco 3640 router, this command is used with the cause-code stats keyword to display the disconnect cause codes that the H.323 subsystem has received. A disconnect can originate either from the far-end gateway or from the opposite call leg on the local gateway. Only the nonzero cause-code counts are displayed.

```
Router# show h323 gateway cause-code stats
CAUSE CODE STATISTICS AT 01:40:25
DISC CAUSE CODE           FROM OTHER PEER      FROM H323 PEER
16 normal call clearing   66                   4976
31 normal, unspecified    1                    0
34 no circuit             31                   0
41 temporary failure      3                    0
44 no requested circuit   13                   0
```

The table below describes significant fields shown in this output

Table 86: show h323 gateway cause-code stats Field Descriptions

Field	Description
Column Headings:	
DISC CAUSE CODE	Decimal value of the cause code, followed by the textual description.
FROM OTHER PEER	Number of disconnects that have been received from the opposite call leg for each cause code (for example, from a PRI T1 POTS peer or a Foreign exchange station [FXS] POTS peer).
FROM H323 PEER	Number of disconnects that have been received from the far-end gateway for each cause code.
Fields listed under the headings are self-explanatory.	

In the following example from a Cisco 3640 router, this command is used with the **h225** keyword to display the cumulative counts of the number of H.225 messages that were sent and received since the counters were last cleared.

Each row shows the sent, received, and failed counts for one type of H.225 request. If the counters have not been cleared, total counts are shown for the router since it was last reloaded.

```
Router# show h323 gateway h225
H.225 STATISTICS AT 00:44:57
H.225 REQUESTS          SENT    RECEIVED    FAILED
Setup                   1654    0           0
Setup confirm           0       1654        0
Alert                   0       828         0
Progress                0       826         0
Call proceeding         0       1654        0
Notify                  0       0           0
Info                    0       0           0
User Info               0       0           0
Facility                0       828         0
Release                 1613    9           1
Reject                  0       0           0
Passthrough             0       0           0
H225 establish timeout  0
RAS failed              1
H245 failed             0
```

The table below describes significant fields shown in this output.

Table 87: show h323 gateway h225 Field Descriptions

Field	Description
Column Headings:	Types of H.225 messages.
H.225 REQUESTS	
SENT	Number of H.225 messages sent by the gateway.
RECEIVED	Number of H.225 messages received from a remote gateway or endpoint.
FAILED	Number of H.225 messages that could not be sent. A failure could occur if, for example, the H.323 subsystem tried to send an H.225 release request but the TCP socket had already been closed.
Fields:	Number of setup messages that were sent, that were received, or that could not be sent. This message is sent by a calling H.323 entity to indicate its desire to set up a connection to the called entity.
Setup	
Setup confirm	Number of setup confirm messages that were sent, that were received, or that could not be sent. This message may be sent by an H.323 entity to acknowledge receipt of a setup message.
Alert	Number of alert messages that were sent, that were received, or that could not be sent. This message may be sent by the called user to indicate that called user alerting has been initiated. (In everyday terms, the "phone is ringing.")

Field	Description
Progress	Number of progress messages that were sent, that were received, or that could not be sent. This message may be sent by an H.323 entity to indicate the progress of a call.
Call proceeding	Number of call proceeding messages that were sent, that were received, or that could not be sent. This message may be sent by the called user to indicate that requested call establishment has been initiated and that no more call establishment information is accepted.
Notify	Number of notify messages that were sent, that were received, or that could not be sent.
Info	Number of information messages that were sent, that were received, or that could not be sent.
User Info	Number of user information messages that were sent, that were received, or that could not be sent. This message may be used to provide additional information for call establishment (for example, overlap signaling), to provide miscellaneous call-related information, or to deliver proprietary features.
Facility	Number of facility messages that were sent, that were received, or that could not be sent. This message is used to provide information on where a call should be directed or for an endpoint to indicate that the incoming call must go through a gatekeeper.
Release	Number of release complete messages that were sent, that were received, or that could not be sent. This message is sent by a gateway to indicate the release of the call if the reliable call signaling channel is open.
Reject	Number of reject messages that were sent, that were received, or that could not be sent.
Passthrough	Number of pass-through messages that were sent, that were received, or that could not be sent.
H225 establish timeout	Number of times the H.323 subsystem was unable to establish an H.225 connection to a remote gateway for a call.
RAS failed	Number of times an Admission Reject (ARJ) or Disengage Reject (DRJ) message is received from the gatekeeper. This counter should equal the arj + drj received counters shown in the show h323 gateway ras command output.
H245 failed	Number of times the H.323 subsystem was unable to create an H.245 tunnel for a call or was unable to send an H.245 message.

In the following example from a Cisco 3640 router, this command is used with the **ras** keyword to display the counters for Registration, Admission, and Status (RAS) messages that were sent to the gatekeeper and received from the gatekeeper. With the exception of the Resource Avail and Req In Progress messages, each RAS message has three variations: a request message, a confirm message, and a reject message. For example, for the Admission message type, there is an Admission Request (arq) message, an Admission Confirm (acf) message, and an Admission Reject (arj) message. The

gateway sends the arq message, and the gatekeeper responds with either an acf or an arj message, depending on whether the gatekeeper confirms or rejects the admission request.

Each of the two tables that follow lists the same message types, with each row showing a different message type. The first table shows the requests sent, the confirms received, and the rejects received. The second table shows the requests received, the confirms sent, and the rejects sent. Some rows in the second table would apply only to the gatekeeper (for example, a gateway would never receive a Registration Request (rrq) message, send a Registration Confirmation (rcf) message, or send a Registration Rejection (rrj) message).

```
Router# show h323 gateway ras
RAS STATISTIC AT 01:10:01
RAS MESSAGE      REQUESTS SENT    CONFIRMS RCVD    REJECTS RCVD
GK Discovery     grq 3            gcf 1            grj 0
Registration     rrq 73           rcf 73           rrj 0
Admission        arq 3216         acf 3215         arj 1
Bandwidth        brq 0            bcf 0            brj 0
Disengage        drq 3174         dcf 3174         drj 0
Unregister       urq 0            ucf 0            urj 0
Resource Avail   rai 0            rac 0
Req In Progress  rip 0
RAS MESSAGE      REQUESTS RCVD    CONFIRMS SENT    REJECTS SENT
GK Discovery     grq 0            gcf 0            grj 0
Registration     rrq 0            rcf 0            rrj 0
Admission        arq 0            acf 0            arj 0
Bandwidth        brq 0            bcf 0            brj 0
Disengage        drq 0            dcf 0            drj 0
Unregister       urq 0            ucf 0            urj 0
Resource Avail   rai 0            rac 0
Req In Progress  rip 0
```

The table below describes significant fields shown in this output.

Table 88: show h323 gateway ras Field Descriptions

Field	Description
Column Headings for the First Table:	
RAS MESSAGE	Type RAS message.
REQUESTS SENT	Number of RAS request messages sent by the gateway to a gatekeeper.
CONFIRMS RCVD	Number of RAS confirmation messages received from a gatekeeper.
REJECTS RCVD	Number of RAS reject messages received from a gatekeeper.
Column Headings for the Second Table:	
RAS MESSAGE	Type of RAS message.
REQUESTS RCVD	Number of RAS request messages received from a gatekeeper.
CONFIRMS SENT	Number of RAS confirmation messages sent by the gateway.
REJECTS SENT	Number of RAS reject messages sent by the gateway.

Field	Description
Fields:	
GK Discovery	Gatekeeper Request (GRQ) message requests that any gatekeeper receiving it respond with a Gatekeeper Confirmation (GCF) message granting it permission to register. The Gateway Reject (GRJ) message is a rejection of this request, indicating that the requesting endpoint should seek another gatekeeper.
Registration	Registration Request (RRQ) message is a request from a terminal to a gatekeeper to register. If the gatekeeper responds with a Registration Confirmation (RCF) message, the terminal uses the responding gatekeeper for future calls. If the gatekeeper responds with a Registration Reject (RRJ) message, the terminal must seek another gatekeeper with which to register.
Admission	Admission Request (ARQ) message requests that an endpoint be allowed access to the packet-based network by the gatekeeper, which either grants the request with an Admission Confirmation (ACF) message or denies it with an Admission Reject (ARJ) message.
Bandwidth	Bandwidth Request (BRQ) message requests that an endpoint be granted a changed packet-based network bandwidth allocation by the gatekeeper, which either grants the request with a Bandwidth Confirmation (BCF) message or denies it with a Bandwidth Reject (BRJ) message.
Disengage	If sent from an endpoint to a gatekeeper, the Disengage Request (DRQ) message informs the gatekeeper that an endpoint is being dropped. If sent from a gatekeeper to an endpoint, the DRQ message forces a call to be dropped; such a request is not refused. The DRQ message is not sent directly between endpoints.
Unregister	UnRegistration Request (URQ) message requests that the association between a terminal and a gatekeeper be broken. Note that the URQ request is bidirectional; that is, a gatekeeper can request a terminal to consider itself unregistered, and a terminal can inform a gatekeeper that it is revoking a previous registration.
Resource Avail	Resource Availability Indication (RAI) message is a notification from a gateway to a gatekeeper of its current call capacity for each H-series protocol and data rate for that protocol. The gatekeeper responds with a Resource Availability Confirmation (RAC) message upon receiving an RAI message to acknowledge its reception.
Req In Progress	Request In Progress (RIP) message can be used by a gateway or gatekeeper when a response to a message cannot be generated within a typical retry timeout period. The RIP message specifies the time period after which a response should have been generated.

Related Commands

Command	Description
show h323 gateway prefixes	Displays the status of the destination-pattern database and the status of the individual destination patterns.

show h323 gateway prefixes

To display the status of the destination-pattern database and the status of the individual destination patterns, use the **show h323 gateway prefixes** command in privileged EXEC mode.

show h323 gateway prefixes

Syntax Description

This command has no arguments or keywords.

Command Default

No default behavior or values

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.2(15)T	This command was introduced.

Usage Guidelines

Use the **show h323 gateway prefixes** command to display the destination patterns from the active plain old telephone service (POTS) dial peers, the current state of the destination pattern (whether they have been sent to or acknowledged by the gatekeeper), and whether advertisement of dynamic prefixes is enabled on the gateway.

Examples

The following command displays the status of the gateway's destination-pattern database:

```
Router# show h323 gateway prefixes
GK Supports Additive RRQ         : True
GW Additive RRQ Support Enabled  : True
Pattern Database Status          : Active
Destination                                      Active
Pattern                          Status          Dial-Peers
=================================================================
1110509*                         ADD ACKNOWLEDGED        2
1110511*                         ADD ACKNOWLEDGED        2
23*                              ADD ACKNOWLEDGED        2
```

The table below describes the significant fields shown in the display.

Table 89: show h323 gateway prefixes Field Descriptions

Field	Description
Pattern Database Status	Status of the gateway's destination-pattern database: active or inactive.

Field	Description
Status	Status of the destination pattern. The status can be one of the following values: ADD PENDING--The gateway has a prefix that is waiting to be sent to the gatekeeper. Prefixes are sent only at the lightweight **registration request**(RRQ) RAS message schedule, which is every 30 seconds. ADD SENT--The gateway sent the prefix to the gatekeeper and is waiting for it to be acknowledged by a registration confirm (RCF) RAS message. ADD ACKNOWLEDGED--The gateway received an RCF message indicating that the gatekeeper accepted the prefix. This is the normal status when dynamic zone prefix registration is working properly. ADD REJECTED--The gatekeeper did not accept the prefix and sent a **registration reject**(RRJ) RAS message. One reason for rejection could be that the gatekeeper already has this prefix registered for a different zone, either by static zone prefix configuration, or because another gateway in a different zone dynamically registered this prefix first. DELETE PENDING--The prefix has gone out of service, for example, because the dial peer shut down, and the gateway is waiting to send an unregistration request (URQ) RAS message to the gatekeeper to remove it. URQ messages are sent at the lightweight RRQ schedule, which is every 30 seconds. DELETE SENT--The gateway sent a URQ message to remove the prefix to the gatekeeper. There is no DELETE ACKNOWLEDGED status. If the prefix is subsequently brought back in service, the status goes back to ADD PENDING.

Related Commands

Command	Description
show h323 gateway	Displays statistics for H.323 gateway messages that have been sent and received and the reasons for which H.l323 calls have been disconnected.

show http client cache

To display information about the entries contained in the HTTP client cache, use the **show http client cache** command in user EXEC or privileged EXEC mode.

show http client cache [**brief**]

Syntax Description

brief	(Optional) Displays summary information about the HTTP client cache.

Command Modes

User EXEC (>)
Privileged EXEC (#)

Command History

Release	Modification
12.2(2)XB	This command was introduced on the Cisco AS5300, Cisco AS5350, and Cisco AS5400.
12.2(11)T	This command was integrated into Cisco IOS Release 12.2(11)T and implemented on the Cisco 3640 and Cisco 3660.
12.4(15)T	The command output was modified to display files cached with URLs of HTTP and HTTPS format in separate tables. The command output was modified to mask out values of the URL attributes when caching of query data returned from the HTTP server is enabled.
12.4(15)XY	A pound sign (#) was added next to the Age field in the command output to indicate entries marked stale manually.
12.4(20)T	This command was integrated into Cisco IOS Release 12.4(20)T

Usage Guidelines

For more information on HTTP caching, see the specification on which it is based: RFC 2616, *Hypertext Transfer Protocol HTTP/1.1,* June 1999, IETF.

Examples

The following is sample output from this command:

```
Router# show http client cache
HTTP Client cached information
==============================
Maximum memory pool allowed for HTTP Client caching = 100000 K-bytes
Maximum file size allowed for caching = 10 K-bytes
Total memory used up for Cache = 18837 Bytes
Message response timeout = 10 secs
Total cached entries     = 5
Total non-cached entries = 0
                             Cached entries
                             ==============
Cached table entry 167,  number of cached entries = 2
 Request URL                             Ref   FreshTime  Age        Size
 -----------                             ---   ---------  ---        ----
 abc.com/vxml/menu.vxml                  0     20         703        319
 abc.com/vxml/opr.vxml                   0     647424     646        2772
Cached table entry 171,  number of cached entries = 1
 Request URL                             Ref   FreshTime  Age        Size
```

```
 -----------                                ---   ---------  ---         ----
 onlineshop.com/catalog/advance.vxml        0     69077      1297649     3453
Cached table entry 172,  number of cached entries = 1
 Request URL                                Ref   FreshTime  Age         Size
 -----------                                ---   ---------  ---         ----
 theater.com/vxml/menu_main.vxml            0     86400      1297661     8734
Cached table entry 176,  number of cached entries = 1
 Request URL                                Ref   FreshTime  Age         Size
 -----------                                ---   ---------  ---         ----
 popcorn.com/menu/selection.vxml            1     20         7           3559
```

In the following example, the **set http client cache stale** command was used to set all the entries in the HTTP client cache to stale. Stale entries are indicated by a pound sign (#) next to the Age field.

```
Router# show http client cache
HTTP Client cached information
==============================
Maximum memory pool allowed for HTTP Client caching = 20000 K-bytes
Maximum file size allowed for caching = 1000 K-bytes
Total memory used up for Cache = 37758 Bytes
Message response timeout = 10 secs
Total cached entries = 7
Total non-cached entries = 0
           Cached entries
           ==============
entry 142, 1 entries
Ref   FreshTime  Age           Size     context
---   ---------  ---           ----     -------
0     30         53233       # 486      63D8FCC4
url: http://goa/TEST1.vxml
entry 145, 1 entries
Ref   FreshTime  Age           Size     context
---   ---------  ---           ----     -------
1     4001998    53218       # 151      0
url: http://win2003/TEST2.vxml
entry 157, 1 entries
Ref   FreshTime  Age           Size     context
---   ---------  ---           ----     -------
1     30         28          # 185      0
url: http://goa/TEST3.vxml
entry 164, 1 entries
Ref   FreshTime  Age           Size     context
---   ---------  ---           ----     -------
1     2231127    53233       # 1183     0
url: http://goa/audio/en_welcome.au
entry 166, 2 entries
Ref   FreshTime  Age           Size     context
---   ---------  ---           ----     -------
1     2231127    53233       # 4916     0
url: http://goa/audio/en_one.au
1     2231127    53229       # 4500     0
url: http://goa/audio/en_three.au
entry 169, 1 entries
Ref   FreshTime  Age           Size     context
---   ---------  ---           ----     -------
1     2231127    53229       # 7224     0
url: http://goa/audio/en_two.au
```

The table below describes the fields shown in this output.

Table 90: show http client cache Field Descriptions

Field	Description
Maximum memory pool allowed for HTTP Client caching	Maximum amount of memory available for the HTTP client to store cached entries in kilobytes. This value is configured by using the **http client cache memory** command.
Maximum file size allowed for caching	Maximum size of a file that can be cached, in kilobytes. If a file exceeds this limit, it cannot be cached. This value is configured by using the **http client cache memory** command.
Total memory used up for Cache	Total amount of memory that is currently being used to store cached entries in kilobytes.
Total cached entries	Total number of cached entries.
Total non-cached entries	Total number of temporary, one-time used HTTP entries that are not currently cached.
Cached table entry	Index marker of the cached table entry. Each cached table entry can contain multiple URLs that were requested and cached.
number of cached entries	Number of URL entries in the cached table entry.
Request URL	URL of the cached entry.
Ref	Whether the cached entry is still in use by the application. 0 means the entry has been freed; 1 or more means that the entry is still being used by that number of applications.
FreshTime	Lifetime of a cached entry, in seconds. When an entry is the same age or older than the refresh time, the entry expires. When a request is made to a cached entry that has expired, the HTTP client sends the server a conditional request for an update. This value is configured on the HTTP server or by using the **http client cache refresh** command on the gateway.
Age	Time for which the entry has been in the cache, in seconds. • Pound sign (#) indicates entries marked stale manually. • Asterisk (*) indicates entries that have become stale without manual intervention.
Size	Size of the cached entry, in bytes.

Related Commands

Command	Description
http client cache memory	Configures the HTTP client cache.
http client cache refresh	Configures the HTTP client cache refresh time.

Command	Description
http client response timeout	Configures the HTTP client server response timeout.
set http client cache stale	Sets the status of all entries in the HTTP client cache to stale.
show http client connection	Displays current HTTP client connection information.

show http client cache

To display information about the entries contained in the HTTP client cache, use the **show http client cache** command in user EXEC or privileged EXEC mode.

show http client cache [**brief**]

Syntax Description

brief	(Optional) Displays summary information about the HTTP client cache.

Command Modes

User EXEC (>)
Privileged EXEC (#)

Command History

Release	Modification
12.2(2)XB	This command was introduced on the Cisco AS5300, Cisco AS5350, and Cisco AS5400.
12.2(11)T	This command was integrated into Cisco IOS Release 12.2(11)T and implemented on the Cisco 3640 and Cisco 3660.
12.4(15)T	The command output was modified to display files cached with URLs of HTTP and HTTPS format in separate tables. The command output was modified to mask out values of the URL attributes when caching of query data returned from the HTTP server is enabled.

Usage Guidelines

For more information on HTTP caching, see the specification on which it is based: RFC 2616, *Hypertext Transfer Protocol HTTP/1.1,* June 1999, IETF.

Examples

The following is sample output from this command:

```
Router# show http client cache
HTTP Client cached information
==============================
Maximum memory pool allowed for HTTP Client caching = 10000 K-bytes (default)
Maximum file size allowed for caching = 50 K-bytes (default)
Total memory used up for Cache = 4271 Bytes
Message response timeout = 10 secs
Total cached entries = 2
Total non-cached entries = 0
Cached entries
           ==============
entry 135, 2 entries
Ref   FreshTime   Age          Size        context
---   ---------   ---          ----        -------
0     121393      557          1419        0
url: http://10.1.200.21/vxml/menu_main.vxml
1     121447      13           2119        0
url: https://10.1.200.21/catalog/advance.vxml
```

The following is sample output from this command when caching of query data returned from the HTTP server is enabled using the http client cache query command. Note that values of the URL attributes are masked out with asterisks (*) to protect caller privacy.

```
Router# show http client cache
HTTP Client cached information
==============================
Maximum memory pool allowed for HTTP Client caching = 10000 K-bytes (default)
Maximum file size allowed for caching = 50 K-bytes (default)
Total memory used up for Cache = 5382 Bytes
Message response timeout = 10 secs
Total cached entries = 4
Total non-cached entries = 0
Cached entries
==============
entry 135, 2 entries
Ref FreshTime Age Size context
--- --------- --- ---- -------
0 121393 577 1419 0
url: http://10.1.200.21/vxml/menu_main.vxml
1 121447 13 2119 0
url: https://10.1.200.21/catalog/advance.vxml
entry 170, 2 entries
Ref FreshTime Age Size context
--- --------- --- ---- -------
0 86400 709 478 67117ABC
url: https://www.somebankurl.com/scripts/login.php?user=*******&password=***
0 86400 528 478 686324C4
url: https://www.somebankurl.com/scripts/login.php?user=********&password=*****
```

The table below describes the fields shown in this output.

Table 91: show http client cache Field Descriptions

Field	Description
Maximum memory pool allowed for HTTP Client caching	Maximum amount of memory available for the HTTP client to store cached entries in kilobytes. This value is configured by using the **http client cache memory**command.
Maximum file size allowed for caching	Maximum size of a file that can be cached, in kilobytes. If a file exceeds this limit, it cannot be cached. This value is configured by using the **http client cache memory**command.
Total memory used up for Cache	Total amount of memory that is currently being used to store cached entries in kilobytes. **Note** In some cases, large files may be cached by two processes. This number is the part of the files cached by the HTTP client process only, so this number may be smaller than the actual size of the files.
Total cached entries	Total number of cached entries.
Total non-cached entries	Total number of temporary, one-time used HTTP entries that are not currently cached.
Cached table entry	Index marker of the cached table entry. Each cached table entry can contain multiple URLs that were requested and cached.
number of cached entries	Number of URL entries in the cached table entry.

Field	Description
Request URL	URL of the cached entry.
Ref	Whether the cached entry is still in use by the application. 0 means the entry has been freed; 1 or more means that the entry is still being used by that number of applications.
FreshTime	Lifetime of a cached entry, in seconds. When an entry is the same age or older than the refresh time, the entry expires. When a request is made to a cached entry that has expired, the HTTP client sends the server a conditional request for an update. This value is configured on the HTTP server or by using the **http client cache refresh**command on the gateway.
Age	Time for which the entry has been in the cache, in seconds.
Size	Size of the cached entry, in kilobytes. **Note** In some cases, large files may be cached by two processes. This number is the part of the file cached by the HTTP client process only, so this number may be smaller than the actual size of the file.

Related Commands

Command	Description
http client cache memory	Configures the HTTP client cache.
http client cache query	Enables caching of query data returned from the HTTP server.
http client cache refresh	Configures the HTTP client cache refresh time.
http client response timeout	Configures the HTTP client server response timeout.
show http client connection	Displays current HTTP client connection information.

show http client cookie

To display cookies that are stored by the HTTP client, use the **show http client cookie** command in privileged EXEC mode.

show http client cookie [**id** *call-id*]

Syntax Description

id *call-id*	(Optional) Displays cookies for the specified call only.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.3(8)T	This command was introduced.

Usage Guidelines

Use the *call-id* argument to display cookies for a specific call; otherwise, this command displays cookies for all calls. Cookies are stored only for the duration of a call. When a call terminates, all associated cookies are deleted. If you use the *call-id* argument and the call is not active, cookies are not displayed and an error message indicates that the call is not active.

Use the **show call active voice brief** command to display the *call-id* for an active call.

Examples

The following is sample output from the **show http client cookie** command:

```
Router# show http client cookie id 144567
HTTP Client Cookies
===================
TestCookieY==password Path=/ Domain=.cisco.com
TestCookieX==username Path=/ Domain=.cisco.com
```

The output lists the name, path, and domain of the cookie. Field descriptions should be self-explanatory.

Related Commands

Command	Description
debug http client cookie	Displays debugging traces related to HTTP cookies.
http client cache memory	Configures the memory limits for the HTTP client cache.
http client cache refresh	Configures the refresh time for the HTTP client cache.
http client cookie	Enables the HTTP client to send and receive and cookies.
show call active voice brief	Displays a call information summary for active calls.
show http client cache	Displays current HTTP client cache information.

show http client history

To display a list of the last 20 requests made by the HTTP client to the server, use the **show http client history** command in user EXEC or privileged EXEC mode.

show http client history

Syntax Description

This command has no arguments or keywords.

Command Modes

User EXEC (>)
Privileged EXEC (#)

Command History

Release	Modification
12.2(2)XB	This command was introduced on the Cisco AS5300, Cisco AS5350, and Cisco AS5400.
12.2(11)T	This command was integrated into Cisco IOS Release 12.2(11)T and implemented on the Cisco 3640 and Cisco 3660.

Usage Guidelines

For more information on HTTP caching, see the specification on which it is based: RFC 2616, *Hypertext Transfer Protocol HTTP/1.1,* June 1999, IETF.

Examples

The following is sample output from this command, showing the most recent GET and POST requests from the HTTP client to the server:

```
Router# show http client history
   POST http://example.com/servlets/account
   GET http://example.com/GetDigit.vxml
   GET http://example.com/form.vxml
   GET http://sample.com/menu.vxml
   POST http://sample.com/servlets/order
   GET http://sample.com/servlets/weather?city=SanFrancisco&state=CA
```

Output shows only requests. There are no field headings.

Related Commands

Command	Description
http client cache memory	Configures the HTTP client cache.
http client response timeout	Configures the HTTP client server response.
show http client connection	Displays current HTTP client connection information.

show http client secure status

To display the trustpoint and cipher suites that are configured in the HTTP client, use the **show http client secure status** command in user EXEC or privileged EXEC mode.

show http client secure status

Syntax Description

This command has no arguments or keywords.

Command Modes

User EXEC (>)

Privileged EXEC (#)

Command History

Release	Modification
12.4(15)T	This command was introduced.
Cisco IOS XE 17.14.1a	This command was modified to display the following TLS v1.3 ciphers: • tls13-aes128-gcm-sha256 • tls13-aes256-gcm-sha384 • tls13-chacha20-poly1305-sha256

Usage Guidelines

This command displays the trustpoint and cipher suites configured in the HTTP client by the **http client secure-trustpoint** and **http client secure-ciphersuite** commands.

Examples

The following sample output displays the configured five cipher suites:

```
Device# show http client secure status

HTTP Client Secure Ciphersuite: rc4-128-md5 rc4-128-sha 3des-cbc-sha des-cbc-sha null-md5
HTTP Client Secure Trustpoint: myca
```

The following sample output displays the configured TLS v1.3 cipher suites:

```
Device# show http client secure status

HTTP Client Secure Ciphersuite: tls13-aes128-gcm-sha256 tls13-aes256-gcm-sha384
tls13-chacha20-poly1305-sha256
HTTP Client Secure Trustpoint: test
```

The following sample output displays the configured default TLS cipher suites:

```
Device# show http client secure status

HTTP Client Secure Ciphersuite: aes-128-cbc-sha rsa-aes-cbc-sha2 dhe-rsa-aes-cbc-sha2
ecdhe-rsa-aes-gcm-sha2
ecdhe-rsa-aes-cbc-sha2 ecdhe-ecdsa-aes-gcm-sha2 tls13-aes128-gcm-sha256
tls13-aes256-gcm-sha384 tls13-chacha20-poly1305-sha256
HTTP Client Secure Trustpoint: ciscoctg-DC1-1A-CA-1
```

The table below describes the significant fields shown in the display.

Table 92: show http client secure status Field Descriptions

Field	Description
HTTP Client Secure Ciphersuite	Cipher suites. • 3des-cbc-sha: Encryption tls_rsa_with_3des_ede_cbc_sha (TLS1.0) ciphersuite • aes-128-cbc-sha: Encryption tls_rsa_with_aes_128_cbc_sha (TLS1.2 & below) ciphersuite • des-cbc-sha: Encryption tls_rsa_with_des_cbc_sha (TLS1.0) ciphersuite • dhe-rsa-aes-cbc-sha2: Encryption tls_rsa_with_cbc_sha2 (TLS1.2) ciphersuite • ecdhe-ecdsa-aes-gcm-sha2: Encryption tls_rsa_with_ecdhe-ecdsa-aes-gcm-sha2 (TLS1.2) ciphersuite • ecdhe-rsa-aes-cbc-sha2: Encryption tls_rsa_with_aes-cbd-sha2 (TLS1.2) ciphersuite • ecdhe-rsa-aes-gcm-sha2: Encryption tls_rsa_with_aes-gcm-sha2 (TLS1.2) ciphersuite • null-md5: Encryption tls_rsa_with_null_md5 (TLS1.0) ciphersuite • rc4-128-md5: Encryption tls_rsa_with_rc4_128_md5 (TLS1.0) ciphersuite • rc4-128-sha; Encryption tls_rsa_with_rc4_128_sha (TLS1.0) ciphersuite • rsa-aes-cbc-sha2: Encryption tls_rsa_with_aes_cbc_sha2 (TLS1.2) ciphersuite • tls13-aes128-gcm-sha256: Encryption tls13_aes128_gcm_sha256 (TLS1.3) ciphersuite • tls13-aes256-gcm-sha384: Encryption tls13_aes256_gcm_sha384 (TLS1.3) ciphersuite • tls13-chacha20-poly1305-sha256: Encryption tls13_chacha20_poly1305_sha256 (TLS1.3) ciphersuite
HTTP Client Secure Trustpoint	Trustpoint name.

Related Commands

Command	Description
http client secure-trustpoint	Declares the trustpoint that the HTTP client will use.
http client secure-ciphersuite	Sets the secure encryption cipher suite for the HTTP client.

show http client statistics

To display information about the communication between the HTTP server and the client, use the **show http client statistics** command in user EXEC or privileged EXEC mode.

show http client statistics

Syntax Description

This command has no arguments or keywords.

Command Modes

User EXEC (>)
Privileged EXEC (#)

Command History

Release	Modification
12.4(15)T	This command was introduced.

Usage Guidelines

Use the data displayed by this command to determine whether the network topology between the HTTP server and client is properly designed and configured. To reset to zero all the counters that collect the information this command displays, use the **clear http client statistics** command.

Examples

The following sample output from this command shows statistics about the communication between the HTTP server and client:

```
Router# show http client statistics
    HTTP Client Statistics:
    =======================
Elapsed time: 759962960 msec
Load Count:
  total load count = 6899220
  total byte count = 26028731394
  largest file size = 624742 bytes
  smallest file size = 374 bytes
Server Response Time to Connect:
  longest response to connect = 10484 msec
  shortest response to connect = 24 msec
Server Response Time to Load:
  longest response to load = 11936 msec
  shortest response to load = 20 msec
File Load Time from Server:
  longest load time = 13124 msec
  shortest load time = 56 msec
Server Connection Count:
  max connections = 23
  established connections = 6901185
Load Rate:
  1 hour : 123300000 bytes
  1 min  : 2055000 bytes
  1 sec  : 34250 bytes
  1 msec : 34.25 bytes
Individual Counts:
  app_requests = 8538451                app_callbacks = 8538451
  200_OK_rsp = 8512959                  other_rsp = 0
  total_errors = 25492                  client_timeouts = 25470
```

```
client_errs = 0                          connect_errs/_timeouts = 7
msg_decode_errs = 0                      msg_encode_errs = 0
msg_xmit_errs = 15                       write_Q_full = 0
socket_rcv_errs = 0                      supported_method_errs = 0
retries = 4645                           late_responses = 0
out_of_memory = 0                        mem_reallocs = 1206
msg_malloced = 0                         event_malloced = 45
cache_freed_by_ager = 1565
```

The table below describes the significant fields shown in the display.

Table 93: show http client statistics Field Descriptions

Field	Description
Elapsed time	Time elapsed since the first HTTP request, in milliseconds (ms).
total load count	Number of API events.
total byte count	Total bytes downloaded from the server by API requests.
largest file size smallest file size	Size of largest and smallest files downloaded from the server, in bytes.
longest response to connect shortest response to connect	Longest and shortest time taken by the server to establish a network connection requested by the client, in ms.
longest response to load shortest response to load	Longest and shortest time taken by the server to fulfill a download request from the client, in ms.
longest load time shortest load time	Longest and shortest time taken by the server to complete downloading the entire file, in ms.
max connections	Maximum concurrent connections.
established connections	Number of currently active and previously established connections.
Load Rate	Downloading rate in bytes/hour, bytes/minute, bytes/second, and bytes/ms.
app_requests	Number of GET and POST requests.
app_callbacks	Number of callbacks to the application.
200_OK_rsp	Number of server messages with response code 200 OK or 304 Not Modified.
other_rsp	Number of server messages with a response code other than 200 and 304.
total_errors	Number of errors encountered by the client.
client_timeouts	Number of timeouts the client has experienced, for example, response timeouts.
client_errs	Number of client internal errors, for example, software errors.
connect_errs/_timeouts	Number of failed or broken connections.

Field	Description
msg_decode_errs	Number of server response messages for which the client failed to decode the headers.
msg_encode_errs	Number of send messages for which the client failed to encode the headers.
msg_xmit_errs	Number of send messages that the client failed to transmit to the server.
write_Q_full	Number of times that the client failed to enter a send message requested by an application into the transmit queue.
socket_rcv_errs	Number of socket read error events returned by TCP.
supported_method_errs	Number of unsupported methods requested by the application.
retries	Number of retransmitted messages.
late_responses	Number of messages that were decoded successfully but exceeded the timeout.
out_of_memory	Number of times that the client failed to allocate memory from Cisco IOS software.
mem_reallocs	Number of times that the client needed to readjust its buffer size because the server response message size exceeded the allocated buffer.
msg_malloced	Number of message buffers currently allocated for receiving messages from the server.
event_malloced	Number of event buffers currently allocated for application programming interface (API) requests.
cache_freed_by_ager	Number of HTTP client cache entries freed up by the background ager process.

Related Commands

Command	Description
clear http client statistics	Resets to zero all the counters that collect the information about the communication between the HTTP server and the client displayed in the output from the **show http client statistics** command.

show interface dspfarm

To display digital-signal-processor (DSP) information on the two-port T1/E1 high-density port adapter for the Cisco 7200 series, use the **show interface dspfarm**command inprivilegedEXEC mode.

show interface dspfarm [*slot/port*] **dsp** [*number*] [**long** | **short**]

Syntax Description

slot	(Optional) Slot location of the port adapter.
/port	(Optional) Port number on the port adapter.
dsp	DSP information.
number	(Optional) Number of DSP sets to show. Range is from 1 to 30.
long	(Optional) Detailed DSP information.
short	(Optional) Brief DSP information.

Command Default

No default behavior or values

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.0(5)XE	This command was introduced on the Cisco 7200 series.
12.1(1)T	This command was integrated into Cisco IOS Release 12.1(1)T.

Usage Guidelines

You can display the local time-division-multiplexing (TDM) cross-connect map by using the following form of this command: **show interface dspfarm <x/y | x/y/z> dsp tdm**..

Examples

The following is sample output from this command for port adapter slot 0 of chassis slot 3 on a Cisco 7200 series router:

```
Router# show interface dspfarm 3/0
DSPfarm3/0 is up, line protocol is up
  Hardware is VXC-2T1/E1
  MTU 256 bytes, BW 12000 Kbit, DLY 0 usec,
     reliability 255/255, txload 4/255, rxload 1/255
  Encapsulation VOICE, loopback not set
  C549 DSP Firmware Version:MajorRelease.MinorRelease (BuildNumber)
     DSP Boot Loader:255.255 (255)
     DSP Application:4.0 (3)
     Medium Complexity Application:3.2 (5)
     High Complexity Application:3.2 (5)
  Total DSPs 30, DSP0-DSP29, Jukebox DSP id 30
  Down DSPs:none
  Total sig channels 120 used 24, total voice channels 120 used 0
     0 active calls, 0 max active calls, 0 total calls
     30887 rx packets, 0 rx drops, 30921 tx packets, 0 tx frags
```

```
   0 curr_dsp_tx_queued, 29 max_dsp_tx_queued
Last input never, output never, output hang never
Last clearing of "show interface" counters never
Queueing strategy:fifo
Output queue 0/0, 0 drops; input queue 0/75, 0 drops
5 minute input rate 13000 bits/sec, 94 packets/sec
5 minute output rate 193000 bits/sec, 94 packets/sec
   30887 packets input, 616516 bytes, 0 no buffer
   Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
   0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
   30921 packets output, 7868892 bytes, 0 underruns
   0 output errors, 0 collisions, 0 interface resets
   0 output buffer failures, 0 output buffers swapped out
```

The table below describes significant fields shown in this output.

Table 94: show interface dspfarm Field Descriptions

Field	Description
DSPfarm3/0 is up	DSPfarm interface is operating. The interface state can be up, down, or administratively down.
Line protocol is	Whether the software processes that handle the line protocol consider the line usable or if it has been taken down by an administrator.
Hardware	Version number of the hardware.
MTU	256 bytes.
BW	12000 kilobits.
DLY	Delay of the interface, in microseconds.
Reliability	Reliability of the interface as a fraction of 255 (255/255 is 100% reliability, calculated as an expediential average over 5 minutes).
Txload	Number of packets sent.
Rxload	Number of packets received.
Encapsulation	Encapsulation method assigned to the interface.
Loopback	Loopback conditions.
C549 DSP Firmware Version	Version of DSP firmware installed.
DSP Boot Loader	DSP boot loader version.
DSP Application	DSP application code version.
Medium Complexity Application	DSP Medium Complexity Application code version.
High Complexity Application	DSP High Complexity Application code version.
Total DSPs	Total DSPs that are equipped in the PA.

Field	Description
DSP0-DSP	DSP number range.
Jukebox DSP id	Jukebox DSP number.
Down DSPs	DSPs not in service.
Total sig channels...used...	Total number of signal channels used.
Total voice channels...used...	Total number of voice channels used.
Active calls	Number of active calls.
Max active calls	Maximum number of active calls.
Total calls	Total number of calls.
Rx packets	Number of received (rx) packets.
Rx drops	Number of rx packets dropped at PA.
Tx packets	Number of transmit (tx) packets.
Tx frags	Number of tx packets that were fragmented.
Curr_dsp_tx_queued	Number of tx packets that are being queued at host DSP queues.
Max_dsp_tx_queued	The max total tx packets that were queued at host DSP queues.
Last input	Number of hours, minutes, and seconds since the last packet was successfully received by an interface. Useful for knowing when a dead interface failed. This counter is updated only when packets are process switched and not when packets are fast switched.
Output	Number of hours, minutes, and seconds since the last packet was successfully sent by the interface. Useful for knowing when a dead interface failed. This counter is updated only when packets are process switched and not when packets are fast switched.
Output hang	Number of hours, minutes, and seconds (or never) since the interface was last reset because of a transmission that took too long. When the number of hours in any of the "last" fields exceeds 24 hours, the number of days and hours is printed. If that field overflows, asterisks (**) are printed.
Last clearing of "show interface" counters	Number of times the "show interface" counters were cleared.
queueing strategy	First-in, first-out queueing strategy (other queueing strategies you might see are priority-list, custom-list, and weighted fair).
Output queue	Number of packets in output queue.
Drops	Number of packets dropped because of a full queue.

Field	Description
Input queue	Number of packets in input queue.
Minute input rate	Average number of bits and packets received per minute in the past 5 minutes.
Bits/sec	Average number of bits sent per second.
Packets/sec	Average number of packets sent per second.
Packets input	Total number of error-free packets received by the system.
Bytes	Total number of bytes, including data and MAC encapsulation, in the error free packets received by the system.
No buffer	Number of received packets discarded because there was no buffer space in the main system. Compare with ignored count. Broadcast storms on Ethernets and bursts of noise on serial lines are often responsible for no-input-buffer events.
Received...broadcasts	Total number of broadcast or multicast packets received by the interface.
Runts	Number of packets that are discarded because they are smaller than the minimum packet size for the medium. For instance, any Ethernet packet that is less than 64 bytes is considered a runt.
Giants	Number of packets that are discarded because they exceed the maximum packet size for the medium. For instance, any Ethernet packet that is greater than 1518 bytes is considered a giant.
Throttles	Number of times the receiver on the port was disabled, possibly because of buffer or processor overload.
Input errors	Number of packet input errors.
CRC	Cyclic redundancy checksum generated by the originating LAN station or far end device does not match the checksum calculated from the data received. On a LAN, this usually indicates noise or transmission problems on the LAN interface or the LAN bus itself. A high number of CRCs is usually the result of collisions or a station sending bad data. On a serial link, CRCs usually indicate noise, gain hits, or other transmission problems on the data link.
Frame	Number of packets received incorrectly having a CRC error and a noninteger number of octets. On a serial line, this is usually the result of noise or other transmission problems.
Overrun	Number of times the serial receiver hardware was unable to hand received data to a hardware buffer because the input rate exceeded the ability of the receiver to handle the data.
Ignore	Number of received packets ignored by the interface because the interface hardware ran low on internal buffers. These buffers are different from the system buffers mentioned previously in the buffer description. Broadcast storms and bursts of noise can cause the ignored count to be incremented.

Field	Description
Abort	Illegal sequence of one bits on the interface.
Packets output	Total number of messages sent by the system.
Bytes	Total number of bytes, including data and MAC encapsulation, sent by the system.
Underruns	Number of times that the far end transmitter has been running faster than the near-end router's receiver can handle.
Output errors	Sum of all errors that prevented the final transmission of datagrams out of the interface being examined. Note that this value might not balance with the sum of the enumerated output errors; some datagrams can have more than one error, and others can have errors that do not fall into any of the specifically tabulated categories.
Collisions	Number of messages re-sent because of an Ethernet collision. Collisions are usually the result of an overextended LAN (Ethernet or transceiver cable too long, more than two repeaters between stations, or too many cascaded multiport transceivers). A packet that collides is counted only once in output packets.
Interface resets	Number of times an interface has been completely reset. Resetting can happen if packets queued for transmission were not sent within a certain interval. If the system notices that the carrier detect line of an interface is up, but the line protocol is down, it periodically resets the interface in an effort to restart it. Interface resets can also occur when an unrecoverable interface processor error occurs, or when an interface is looped back or shut down.
Output buffer failures	Number of failed buffers.
Output buffers swapped out	Number of buffers swapped out.

Related Commands

Command	Description
show interfaces	Displays statistics for all interfaces configured on the router or access server.

show interfaces cable-modem

To display statistics for all interfaces configured on the cable modem port and to define Hybrid Fiber-Coax (HFC) statistics on the modem, use the **show interfaces cable-modem** command in privileged EXEC mode.

show interfaces cable-modem *port*

Syntax Description

port	The port number.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.4(11)T	This command was introduced.

Usage Guidelines

This command can be used to define the HFC state on the modem.

Examples

The following example shows the HFC state on the modem. The resulting output varies, depending on the network for which an interface has been configured.

```
Router# show interfaces cable-modem 0/1/0

cable-modem0/1/0 is up, line protocol is up
  HFC state is OPERATIONAL, HFC MAC address is 00d0.59e1.2073
  Hardware is Cable modem, address is 0014.f26d.10b2 (bia 0014.f26d.10b2)
  Internet address is 00.0.0.01/1
  MTU 1500 bytes, BW 1544 Kbit, DLY 6470 usec,
     reliability 255/255, txload 247/255, rxload 246/255
  Encapsulation ARPA, loopback not set
  ARP type: ARPA, ARP Timeout 04:00:00
  Last input 00:00:01, output 00:00:00, output hang never
  Last clearing of "show interface" counters 00:07:03
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 83594
  Queueing strategy: Class-based queueing
  Output queue: 61/1000/64/83594 (size/max total/threshold/drops)
     Conversations  2/5/256 (active/max active/max total)
     Reserved Conversations 0/0 (allocated/max allocated)
     Available Bandwidth 232 kilobits/sec
  30 second input rate 2581000 bits/sec, 987 packets/sec
  30 second output rate 1585000 bits/sec, 639 packets/sec
  HFC input: 0 errors, 0 discards, 0 unknown protocols 0 flow control discards
  HFC output: 0 errors, 0 discards
     304582 packets input, 105339474 bytes, 0 no buffer
     Received 0 broadcasts, 0 runts, 0 giants, 1 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
     0 input packets with dribble condition detected
     228195 packets output, 78392605 bytes, 0 underruns
     0 output errors, 0 collisions, 1 interface resets
     0 babbles, 0 late collision, 0 deferred
     0 lost carrier, 0 no carrier
     0 output buffer failures, 0 output buffers swapped out
```

The table below describes the significant fields shown in the display.

Table 95: show interfaces cable-modem Field Descriptions

HFC State Values	Description
HFC state is OPERATIONAL	Current HFC state on the modem.
HFC MAC address	The HFC MAC address for this modem.
Hardware is Cable modem	Hardware type.
Internet address	The IP address for this modem.
MTU	Total MTU usage in bytes, kilobits, user seconds. Describes reliability, transmit load, and receiver load.
Encapsulation ARPA, loopback not set	Encapsulation type and whether loopback is set.
ARP type: ARPA, ARP Timeout	ARP type and timeout parameters.
Last input, output, output hang	Most recent input and output statistics.
Last clearing of "show interface" counters	Most recent usage of **show interface** command counters.
Input queue, Total output drops	Input queue and output drop statistics in the following format: size/max/drops/flushes.
Queueing strategy: Class-based queueing	Queueing type. In this case, class-based queueing.
Output queue	Output queue statistics in the following format: size/max total/threshold/drops.
Conversations	Type and number of conversations in the following format: active/max active/max total.
Reserved Conversations	Number of reserved conversations in the following format: allocated/max allocated.
Available Bandwidth	Allotted bandwidth in kilobits per second.
input rate, packets	Input rate and number of packets in bits per second, packets per second.
output rate, packets	Output rate and number of packets in bits per second, packets per second.
HFC input, output	HFC input statistics in the following format: errors, discards, unknown protocols, flow control discards.
packets input	Number of packets in bytes, with or without buffer.
Received broadcasts, runts, giants, throttles	Number of broadcasts, runts, giants, and throttles.
input errors	Number and type of input errors in the following format: cyclic redundancy check (CRC), frame, overrun, ignored.
packets output	Number of packets output in bytes and underruns.

HFC State Values	Description
output errors, collisions, interface resets	Number of output errors, collisions, and interface resets.
babbles, late collision, deferred	Number of babbles, late collisions, and deferred packets.
lost carrier, no carrier	Carrier statistics.
output buffer failures, output buffers swapped out	Buffer statistics.

The HFC state is the Data Over Cable Service Interface Specification (DOCSIS) state for the cable modem connection to the cable modem termination system (CMTS). The table below describes HFC state values.

Table 96: HFC State Values

HFC State Values	Description
NOT_READY	Cable modem controller is resetting.
NOT_SYNCHRONIZED	Cable modem controller is starting the downstream frequency scan.
PHY_SYNCHRONIZED	Cable modem controller locked the downstream signal and is collecting the upstream channel parameter information.
US_PARAMETERS_ACQUIRED	Cable modem controller collected upstream channel parameter information and is trying to lock upstream frequency.
RANGING_COMPLETE	Cable modem controller received the CMTS range response, has finished downstream/upstream lock process, and is initializing IP.
IP_COMPLETE	Cable modem controller has IP information.
WAITING_FOR_DHCP_OFFER	Cable modem controller is sending a Dynamic Host Configuration Protocol (DHCP) request to the CMTS.
WAITING_FOR_DHCP_RESPONSE	Cable modem controller is waiting for a DHCP response from the CMTS.
WAITING_FOR_TIME_SERVER	Cable modem controller is starting the time of day (ToD) service.
TOD_ESTABLISHED	Cable modem controller has received the ToD packet and has synchronized its local time.
WAITING_FOR_TFTP	Cable modem controller is downloading its running configuration from the CMTS-defined TFTP server.
PARAM_TRANSFER_COMPLETE	Cable modem controller has completed transferring its running configuration.
REGISTRATION_COMPLETE	Cable modem controller has sent out its registration request, and CMTS has accepted it.

HFC State Values	Description
REFUSED_BY_CMTS	Cable modem controller registration request has been rejected by CMTS.
FORWARDING_DENIED	Cable modem controller registration to CMTS was successful, but network access is disabled in the running configuration.
OPERATIONAL	Cable modem controller is ready for service.
UNKNOWN	Cable modem controller is an undefined state

The table below lists input error descriptions.

Table 97: Input Error Description

Input Error	Description
errors	The total number of input packets discarded on the cable modem controller.
discards	The number of input packets discarded due to a momentary lack of resources.
unknown protocols	The number of input packets discarded because they have unsupported or unknown protocol values.
flow control discards	The number of input packets discarded because the cable modem controller overflowed transferring packets to the router.

The table below lists output error descriptions.

Table 98: Output Error Description

Output Error	Description
errors	Total number of output packets discarded on the cable modem controller.
discards	Total number of output packets discarded due to a momentary lack of resources.

Related Commands

Command	Description
show interfaces	Displays statistics for all interfaces.

show ip address trusted check

To check the trust of a call setup from a VoIP source, use the **show ip address trusted check** command in privileged EXEC mode.

show ip address trusted check {*IPv4 address IPv6 address*}

Syntax Description

IPv4 address/IPv6 address	IP address of the VoIP source that initiated the call setup.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
IOS XE Fuji Release 16.8.1	This command was introduced.

Usage Guidelines

Use the **show ip address trusted check** command from the Toll-fraud prevention support feature, to check the trust of the incoming H.323 or SIP trunk calls. The IP address authentication validates the trust of the incoming call.

This command checks the IP address trusted list and the authentication is passed when an entry matches with source IP address. To display the IP address trusted list, use the **show ip address trusted list** command in privileged EXEC mode.

Example

The following example shows the IP address authentication passed for the VoIP source 15.1.0.1.

```
Router# show ip address trusted check 15.1.0.1
ip[15.1.0.1] authenticate is PASSED by peer ip addr
```

The following example shows the IP address authentication failed for the VoIP source 15.3.0.1.

```
Router# show ip address trusted check 15.3.0.1
ip[15.3.0.1] authentication is FAILED!
```

Related Commands

Command	Description
show ip address trusted list	Displays the IP address trusted list.
ip address trusted	Enables toll-fraud prevention support on a device.

show iua as

To display information about the current condition of an application server (AS), use the **show iua as** command in privileged EXEC mode.

show iua as {**all** | **name** *as-name*}

Syntax Description

all	Output displays information about all configured ASs.
name *as -name*	Name of a particular AS. Output displays information about just that AS.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.2(4)T	This command was introduced.
12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T. Support for the Cisco AS5300, Cisco AS5350, Cisco AS5400, and Cisco AS5850 is not included in this release.
12.2(11)T	This command was implemented on the Cisco 2420, Cisco 2600 series, Cisco 3600 series, Cisco 3700 series, Cisco AS5300, Cisco AS5350, Cisco AS5400, and Cisco AS5850.

Usage Guidelines

Use the **show iua as all** command to find the failover timer value. You need to know the current failover timer value before you changeit to fit your application.

Examples

The following sample output from this command shows that the current state of the AS (as1) is active and that there are four PRI interfaces configured to use this AS:

```
Router# show iua as all
Name of AS :as1
        Total num of ASPs configured :2
                asp1
                asp2
        Current state :  ACTIVE
        Active ASP :asp1
        Number of ASPs up :1
        Fail-Over time : 4000 milliseconds
        Local address list : 10.1.2.345 10.2.3.456
        Local port:2139
        Interface IDs registered with this AS
                 Interface ID
                 0 (Dchannel0)
                 3 (Dchannel3)
                 2 (Dchannel2)
                 1 (Dchannel1)
```

The table below describes significant fields shown in the output.

Table 99: show iua as all Field Descriptions

Field	Description
Name of AS: 1	Name of the AS.
Total num of ASPs configured :2 asp1 asp2	Total number of application server processes (ASPs) configured.
Current state : ACTIVE	The possible states are ACTIVE, INACTIVE, and DOWN.
Active ASP :asp1	Shows the active ASP.
Number of ASPs up :1	If two ASPs are up, then the one that is not active is in standby mode.
Fail-Over time : 4000 milliseconds	Default is 4000 ms, although the value can also be configured through the CLI under AS.
Local address list : 10.1.2.345 10.2.3.456	Configured by the user.
Local port:2139	Configured by the user.
Interface IDs registered with this AS Interface id 0 (Dchannel0) 3 (Dchannel3) 2 (Dchannel2) 1 (Dchannel1)	The D channels that are bound to this AS.

Related Commands

Command	Description
clear ip sctp statistics	Clears statistics counts for SCTP.
show ip sctp association list	Displays a list of all current SCTP associations.
show ip sctp association parameters	Displays the parameters configured for the association defined by the association ID.
show ip sctp association statistics	Displays the current statistics for the association defined by the association ID.
show ip sctp errors	Displays error counts logged by SCTP.
show ip sctp instances	Displays the currently defined SCTP instances.
show ip sctp statistics	Displays the overall statistics counts for SCTP.
show isdn	Displays information about memory, Layer 2 and Layer 3 timers, and the status of PRI channels.

Command	Description
show iua asp	Displays information about the current condition of an ASP.

show iua asp

To display information about the current condition of an application server process (ASP), use the **show iua asp** command in privileged EXEC mode.

show iua asp {**all** | **name** *asp-name*}

Syntax Description

all	Displays information about all configured ASPs.
name *asp -name*	Name of a particular ASP. Displays information about just that ASP.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.2(4)T	This command was introduced.
12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T. Support for the Cisco AS5300, Cisco AS5350, Cisco AS5400, and Cisco AS5850 is not included in this release.
12.2(11)T	This command was implemented on the Cisco AS5300.
12.2(15)T	This command was integrated into Cisco IOS Release 12.2(15)T on the Cisco 2420, Cisco 2600 series, Cisco 3600 series, and Cisco 3700 series; and Cisco AS5300, Cisco AS5350, Cisco AS5400, and Cisco AS5850 network access server (NAS) platforms.

Usage Guidelines

This command establishes Stream Control Transmission Protocol (SCTP) associations. There can only be a maximum of two ASPs configured per application server (AS).

Examples

The following typical output for the **show iua asp all** command shows that the current state of the ASP (asp1) is active. This command also gives information about the SCTP association being used by this ASP.

```
Router# show iua asp all
Name of ASP :asp1
Current State of ASP:ASP-Active
Current state of underlying SCTP Association IUA_ASSOC_ESTAB , assoc  id 0
SCTP Association information :
         Local Receive window :9000
         Remote Receive window :9000
         Primary Dest address requested by IUA 10.11.2.33
         Effective Primary Dest address 10.11.2.33
Remote  address list :10.22.3.44
Remote Port :9900
Statistics :
        Invalid SCTP signals Total :0  Since last  0
        SCTP Send failures :0
```

The table below describes significant fields shown in this output.

Table 100: show iua asp all Field Descriptions

Field	Description
Name of ASP: 1	Name of the application server process (ASP).
Current State of ASP: ASP-Active	The possible states are ACTIVE, INACTIVE, and DOWN.
Current state of underlying SCTP Association IUA_ASSOC_ESTAB , assoc id 0	States used for underlying SCTP association: IUA_ASSOC_ESTAB (association established) or IUA_ASSOC_INIT (association not established...attempting to initiate).
SCTP Association information : Local Receive window :9000 Remote Receive window :9000	Configured by the user.
Primary Dest address requested by IUA 10.11.2.33	The IP address through which the current link is established.
Remote address list :10.22.3.44 Remote Port :9900	Configured by the user.
Statistics : Invalid SCTP signals Total :0 Since last 0 SCTP Send failures :0	Information useful for seeing if errors are happening with the SCTP connection.

Related Commands

Command	Description
clear ip sctp statistics	Clears statistics counts for SCTP.
show ip sctp association list	Displays a list of all current SCTP associations.
show ip sctp association parameters	Displays the parameters configured for the association defined by the association ID.
show ip sctp association statistics	Displays the current statistics for the association defined by the association ID.
show ip sctp errors	Displays error counts logged by SCTP.
show ip sctp instances	Displays the currently defined SCTP instances.
show ip sctp statistics	Displays the overall statistics counts for SCTP.
show iua as	Displays information about the current condition of an AS.

show media-proxy sessions

To display the details of an active or completed SIP recording sessions on the CUBE Media Proxy, use the **show media-proxy sessions** command in privileged EXEC mode.

show media-proxy sessions [**summary** [**history**] | **call-id** *call-id* | **session-id** *WORD* | **metadata-session-id** *x-session-id*]

Syntax Description

summary	(Optional) Displays the summary of the active SIP recording sessions.
history	(Optional) Displays the summary of the completed SIP recording sessions.
call-id *call-id*	(Optional) Displays the details of the inbound and forked legs that are associated with the specified CCAPI call identifier of the SIP leg.
session-id *WORD*	(Optional) Displays the details of the Media Proxy recording sessions that are associated with the specified session-id.
metadata-session-id *x-session-id*	(Optional) Displays the details of the Media Proxy recording sessions that are associated with the x-session-id present in the "From" header of the INVITE from CUCM.

Command Default

Displays active recording session details.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Gibraltar Release 16.10.1a	This command was introduced.
Cisco IOS XE Amsterdam 17.3.1a	The output of the command **show media-proxy sessions** was modified to include "SIPREC" field.

Usage Guidelines

The command **show media-proxy sessions** displays recording session details such as inbound call-ID, forked call-ID, session-ID, dial-peer tags, IP, port number, total sessions, and failed recording sessions.

You can also get details of a specific SIP leg call-ID. MSP call-ID is not a valid value for this command.

Example

The following example shows the sample output for **show media-proxy sessions**.

```
Device# show media-proxy sessions

No.   Call-ID          Session-ID                          Dialpeer   Secure   SIPREC
      Inbound/Forked   LocalUuid;RemoteUuid                Tag        (Y/N)    (Y/N)
=============================================================================================
1     36770/-          a234a20672ce596d969c59ee9767f127;   3           N        Y
                       aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
```

The following example shows the details for the active recording sessions.

```
Device# show media-proxy sessions summary

 No       Inbound/Forked      Dialpeer-Tag          IP:Port          Total/Failed Sessions
-------------------------------------------------------------------------------------------

 1         Forked               100          ipv4:8.0.0.200:6680             2/0
 2         Forked               200          ipv4:8.0.0.200:6220             2/0
 3         Inbound             5678                                          2/0
```

The following example shows the details for the completed recording sessions.

```
Device# show media-proxy sessions summary history

 No.      Inbound/Forked     Dialpeer Tag         IP:Port             Total/Failed Sessions
-------------------------------------------------------------------------------------------

 1         Inbound             5678                                         2/0
 2         Forked               100          ipv4:8.0.0.200:6680            2/0
 3         Forked               200          ipv4:8.0.0.200:6220            2/0
```

The following example shows the details of a specified SIP leg call-ID.

```
Device# show media-proxy sessions call-id 2

CC Call-ID: 1 Inbound-leg
Dur: 00:00:15 tx: 0/0 rx: 1484/296800 lost: 0/0/0 delay: 0/0/0ms
Remote-Addr: 8.41.17.71:6009 Local-Addr: 8.43.33.203:8000 rtt:0ms pl:0/0ms
Dialpeer-Tag: 100 Negotiated-Codec: g711ulaw
SRTP-Status: off SRTP-Cipher: NA
LocalUUID: 6bde661e9767590b930f3427ad6e94e9 RemoteUUID: aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa

CC Call-ID: 2 Forked-leg (Primary)
Dur: 00:00:15 tx: 1484/296800 rx: 0/0 lost: 0/0/0 delay: 0/0/0ms
Remote-Addr: 8.41.17.71:6000 Local-Addr: 8.43.33.203:8002 rtt:0ms pl:0/0ms
Dialpeer-Tag: 200 Negotiated-Codec: g711ulaw
SRTP-Status: off SRTP-Cipher: NA
LocalUUID: bbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbb RemoteUUID: 6bde661e9767590b930f3427ad6e94e9

CC Call-ID: 7 Forked-leg
Dur: 00:00:15 tx: 1480/296000 rx: 0/0 lost: 0/0/0 delay: 0/0/0ms
Remote-Addr: 8.41.17.71:6001 Local-Addr: 8.43.33.203:8004 rtt:0ms pl:0/0ms
Dialpeer-Tag: 300 Negotiated-Codec: g711ulaw
SRTP-Status: off SRTP-Cipher: NA
LocalUUID: cccccccccccccccccccccccccccccccc RemoteUUID: 6bde661e9767590b930f3427ad6e94e9

CC Call-ID: 9 Forked-leg
Dur: 00:00:15 tx: 1479/295800 rx: 0/0 lost: 0/0/0 delay: 0/0/0ms
Remote-Addr: 8.41.17.71:6004 Local-Addr: 8.43.33.203:8006 rtt:0ms pl:0/0ms
Dialpeer-Tag: 400 Negotiated-Codec: g711ulaw
SRTP-Status: off SRTP-Cipher: NA
LocalUUID: cccccccccccccccccccccccccccccccc RemoteUUID: 6bde661e9767590b930f3427ad6e94e9

CC Call-ID: 11 Forked-leg
Dur: 00:00:15 tx: 1479/295800 rx: 0/0 lost: 0/0/0 delay: 0/0/0ms
Remote-Addr: 8.41.17.71:6005 Local-Addr: 8.43.33.203:8008 rtt:0ms pl:0/0ms
Dialpeer-Tag: 500 Negotiated-Codec: g711ulaw
SRTP-Status: off SRTP-Cipher: NA
LocalUUID: cccccccccccccccccccccccccccccccc RemoteUUID: 6bde661e9767590b930f3427ad6e94e9

CC Call-ID: 13 Forked-leg
Dur: 00:00:15 tx: 1479/295800 rx: 0/0 lost: 0/0/0 delay: 0/0/0ms
```

```
Remote-Addr: 8.41.17.71:6008 Local-Addr: 8.43.33.203:8010 rtt:0ms pl:0/0ms
Dialpeer-Tag: 600 Negotiated-Codec: g711ulaw
SRTP-Status: off SRTP-Cipher: NA
LocalUUID: ccccccccccccccccccccccccccccccc RemoteUUID: 6bde661e9767590b930f3427ad6e94e9
```

The following example shows the details of a specified session-id.

```
Device# show media-proxy sessions session-id 6bde661e9767590b930f3427ad6e94e9
CC Call-ID: 1 Inbound-leg
Dur: 00:00:15 tx: 0/0 rx: 1484/296800 lost: 0/0/0 delay: 0/0/0ms
Remote-Addr: 8.41.17.71:6009 Local-Addr: 8.43.33.203:8000 rtt: 0ms pl: 0/0ms
Dialpeer-Tag: 100 Negotiated-Codec: g711ulaw
SRTP-Status: off SRTP-Cipher: NA
LocalUUID: 6bde661e9767590b930f3427ad6e94e9 RemoteUUID: aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa

CC Call-ID: 2 Forked-leg (Primary)
Dur: 00:00:15 tx: 1484/296800 rx: 0/0 lost: 0/0/0 delay: 0/0/0ms
Remote-Addr: 8.41.17.71:6000 Local-Addr: 8.43.33.203:8002 rtt: 0ms pl: 0/0ms
Dialpeer-Tag: 200 Negotiated-Codec: g711ulaw
SRTP-Status: off SRTP-Cipher: NA
LocalUUID: bbbbbbbbbbbbbbbbbbbbbbbbbbbbbbb RemoteUUID: 6bde661e9767590b930f3427ad6e94e9

CC Call-ID: 7 Forked-leg
Dur: 00:00:15 tx: 1480/296000 rx: 0/0 lost: 0/0/0 delay: 0/0/0ms
Remote-Addr: 8.41.17.71:6001 Local-Addr: 8.43.33.203:8004 rtt: 0ms pl: 0/0ms
Dialpeer-Tag: 300 Negotiated-Codec: g711ulaw
SRTP-Status: off SRTP-Cipher: NA
LocalUUID: ccccccccccccccccccccccccccccccc RemoteUUID: 6bde661e9767590b930f3427ad6e94e9

CC Call-ID: 9 Forked-leg
Dur: 00:00:15 tx: 1479/295800 rx: 0/0 lost: 0/0/0 delay: 0/0/0ms
Remote-Addr: 8.41.17.71:6004 Local-Addr: 8.43.33.203:8006 rtt: 0ms pl: 0/0ms
Dialpeer-Tag: 400 Negotiated-Codec: g711ulaw
SRTP-Status: off SRTP-Cipher: NA
LocalUUID: ccccccccccccccccccccccccccccccc RemoteUUID: 6bde661e9767590b930f3427ad6e94e9

CC Call-ID: 11 Forked-leg
Dur: 00:00:15 tx: 1479/295800 rx: 0/0 lost: 0/0/0 delay: 0/0/0ms
Remote-Addr: 8.41.17.71:6005 Local-Addr: 8.43.33.203:8008 rtt: 0ms pl: 0/0ms
Dialpeer-Tag: 500 Negotiated-Codec: g711ulaw
SRTP-Status: off SRTP-Cipher: NA
LocalUUID: ccccccccccccccccccccccccccccccc RemoteUUID: 6bde661e9767590b930f3427ad6e94e9

CC Call-ID: 13 Forked-leg
Dur: 00:00:15 tx: 1479/295800 rx: 0/0 lost: 0/0/0 delay: 0/0/0ms
Remote-Addr: 8.41.17.71:6008 Local-Addr: 8.43.33.203:8010 rtt: 0ms pl: 0/0ms
Dialpeer-Tag: 600 Negotiated-Codec: g711ulaw
SRTP-Status: off SRTP-Cipher: NA
LocalUUID: ccccccccccccccccccccccccccccccc RemoteUUID: 6bde661e9767590b930f3427ad6e94e9
```

The following example shows the details of Media Proxy recording sessions based on the x-session-id that is present in the "From" header of the INVITE from CUCM.

```
Device# show media-proxy sessions metadata-session-id 696dd5d3f7755c6abdc438e93d01febf
CC Call-ID: 77 Inbound-leg
Dur: 00:00:46 tx: 0/0 rx: 3105/578880 lost: 0/0/0 delay: 0/0/0ms
Remote-Addr: 8.0.0.200:8010 Local-Addr: 8.43.33.203:8048 rtt: 0ms pl: 0/0ms
Dialpeer-Tag: 1 Negotiated-Codec: g711ulaw
SRTP-Status: off SRTP-Cipher: NA
LocalUUID: 528b282b804c5fd098eaba3696c00de2 RemoteUUID: aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa

CC Call-ID: 78 Forked-leg (Primary)
Dur: 00:00:46 tx: 3105/578880 rx: 0/0 lost: 0/0/0 delay: 0/0/0ms
```

```
Remote-Addr: 8.0.0.200:8014 Local-Addr: 8.43.33.203:8050 rtt: 0ms pl: 0/0ms
Dialpeer-Tag: 2 Negotiated-Codec: g711ulaw
SRTP-Status: off SRTP-Cipher: NA
LocalUUID: bbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbb RemoteUUID: 528b282b804c5fd098eaba3696c00de2

CC Call-ID: 84 Forked-leg
Dur: 00:00:46 tx: 3100/577880 rx: 0/0 lost: 0/0/0 delay: 0/0/0ms
Remote-Addr: 8.0.0.200:8018 Local-Addr: 8.43.33.203:8052 rtt: 0ms pl: 0/0ms
Dialpeer-Tag: 3 Negotiated-Codec: g711ulaw
SRTP-Status: off SRTP-Cipher: NA
LocalUUID: bbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbb RemoteUUID: 528b282b804c5fd098eaba3696c00de2

CC Call-ID: 86 Forked-leg
Dur: 00:00:46 tx: 3101/578080 rx: 0/0 lost: 0/0/0 delay: 0/0/0ms
Remote-Addr: 8.0.0.200:8022 Local-Addr: 8.43.33.203:8054 rtt: 0ms pl: 0/0ms
Dialpeer-Tag: 4 Negotiated-Codec: g711ulaw
SRTP-Status: off SRTP-Cipher: NA
LocalUUID: bbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbb RemoteUUID: 528b282b804c5fd098eaba3696c00de2

CC Call-ID: 88 Forked-leg
Dur: 00:00:46 tx: 3101/578080 rx: 0/0 lost: 0/0/0 delay: 0/0/0ms
Remote-Addr: 8.0.0.200:8026 Local-Addr: 8.43.33.203:8056 rtt: 0ms pl: 0/0ms
Dialpeer-Tag: 5 Negotiated-Codec: g711ulaw
SRTP-Status: off SRTP-Cipher: NA
LocalUUID: bbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbb RemoteUUID: 528b282b804c5fd098eaba3696c00de2

CC Call-ID: 91 Forked-leg
Dur: 00:00:46 tx: 3101/578080 rx: 0/0 lost: 0/0/0 delay: 0/0/0ms
Remote-Addr: 8.0.0.200:8030 Local-Addr: 8.43.33.203:8058 rtt: 0ms pl: 0/0ms
Dialpeer-Tag: 6 Negotiated-Codec: g711ulaw
SRTP-Status: off SRTP-Cipher: NA
LocalUUID: bbbbbbbbbbbbbbbbbbbbbbbbbbbbbbbb RemoteUUID: 528b282b804c5fd098eaba3696c00de2
```

show media resource status

To display the current media resource status, use the **show media resource status** command in privileged EXEC mode.

show media resource status

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.3(8)T	This command was introduced.

Examples

The following example displays the current media resource status:

```
Router# show media resource status
 Resource Providers:
 Resource  Provider ID :: FLEX_DSPRM Status :: REGISTERED
 Service Profiles
 MTP ::
 TRANSCODING :: 6 11
 CONFERENCING :: 10
 Applications :
 Application ID : SCCP, Status : REGISTERED
```

The table below describes significant fields shown in this output.

Table 101: show media resource status Field Descriptions

Field	Description
MTP	Displays the profile numbers configured for MTP resources.
TRANSCODING	Displays the profile numbers configured for transcoding resources.
CONFERENCING	Displays the profile numbers configured for conferencing resources.
Status	Displays the current status of the profile.

Related Commands

Command	Description
dsp services dspfarm	Configures DSP farm services for a specified voice card.
dspfarm profile	Enters DSP farm profile configuration mode and defines a profile for DSP farm services.
show dspfarm profile	Displays configured DSP farm profile information for a Cisco CallManager group.

show mediacard

To display configuration information about media card conferencing, transcoding, Media Termination Points (MTPs) and Digital Signal Processors (DSPs), use the **show mediacard** command in privileged EXEC mode.

show mediacard slot [**conference** | **connections** | **dsp** *number*]

Syntax Description

slot	Specifies the slot number of the card to be displayed. Valid values are from 1 to 4.
conference	(Optional) Displays information on ad-hoc conferences.
connections	(Optional) Displays information on media card connections.
dsp *number*	(Optional) Displays information on the specified DSP resource pool. The *number*argument ranges in value from 1 to 4.

Command Default

No default behavior or values

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.3(8)XY	This command was introduced on the Communication Media Module.
12.3(14)T	This command was integrated into Cisco IOS Release 12.3(14)T.
12.4(3)	This command was integrated into Cisco IOS Release 12.4(3).

Usage Guidelines

Use this command to display media card status, statistics, and configuration information.

Examples

The following is sample output for the **show mediacard** command:

```
Router# show mediacard 3
Media Card 3: WS-SVC-CMM-ACT
 Service: Adhoc/Meetme conference and MTP/Transcoding
 State: ENABLE
 DSP image version (all DSPs): 1.1(06), build: 1.1(06)
 DSP status:
  DSP 1 | DSP 2 | DSP 3 | DSP 4
 -------|-------|-------|-------
  alive | alive | alive | alive
 Total 128 DSP channels, 1 active
 Resource pools                     | DSPs | Used by Active profile
 -----------------------------------|------|-----------------------
  Pool1                              |  2   |  1
  Pool2                              |  1   |
  Pool3                              |  1   |  2
Router# show mediacard 3 dsp 3
DSP image version (all DSPs): 1.1(06), build: 1.1(06)
 Card DSP status Chan status RxPkts TxPkts
  3   3   alive  1    idle   -      -
```

```
                    2    idle   -      -
                    3    idle   -      -
                    4    idle   -      -
                    5    idle   -      -
                    6    idle   -      -
                    7    idle   -      -
                    8    idle   -      -
                    9    idle   -      -
                    10   idle   -      -
                    11   idle   -      -
                    12   idle   -      -
                    13   idle   -      -
                    14   idle   -      -
                    15   idle   -      -
                    16   idle   -      -
                    17   idle   -      -
                    18   idle   -      -
                    19   idle   -      -
                    20   idle   -      -
                    21   idle   -      -
                    22   idle   -      -
                    23   idle   -      -
                    24   idle   -      -
                    25   idle   -      -
                    26   idle   -      -
                    27   idle   -      -
                    28   idle   -      -
                    29   idle   -      -
                    30   idle   -      -
                    31   idle   -      -
                    32   idle   -      -
 Total 32 DSP channels, 0 active
Router# show mediacard conference
Id  Slot/  RxPkts TxPkts RPort SPort Remote-Ip
    DSP/Ch
0   2/4/1 32024     16498    27004 27020  10.7.16.87
0   2/4/2 17368     17192    17582 17583  10.7.16.80
0   2/4/3 21904     16990    26155 26168  10.7.16.94
Total: 3
Router# show mediacard connections
Id  Type  Slot/  RxPkts TxPkts RPort SPort Remote-Ip
          DSP/Ch
0   conf  3/4/1  24028  16552 0      0      10.7.16.87
Total: 1
Router# show mediacard connections
Id  Type  Slot/  RxPktsTxPktsRPort SPort Remote-Ip
          DSP/Ch
0   mtp   3/1/1  16544 16488 1046   1046   10.1.2.15
0   mtp   3/1/2  19396 19662 1046   1046   10.1.80.50
0   mtp   3/1/3  17562 20122 626    626    10.1.2.15
0   mtp   3/1/4  17488 17328 626    626    10.1.80.5
```

The table below describes the significant fields shown in the display.

Table 102: show mediacard Field Descriptions

Field	Description
RxPkts	Number of packets transmitted
TxPkts	Number of packets received
RPort	Receiving port

Field	Description
SPort	Sending port
Remote-Ip	IP address of the remote endpoint

Related Commands

Command	Description
debug mediacard	Displays debugging information for DSPRM.

show mgcp

To display values for Media Gateway Control Protocol (MGCP) parameters, use the **show mgcp** command in user EXEC or privileged EXEC mode.

show mgcp [**connection** | **endpoint** | **nas** {**dump** *slot port chan-number* | **info**} | **notify-entity** | **profile** [*name*] | **statistics**]

Syntax Description

connection	(Optional) Displays the active MGCP-controlled connections.
endpoint	(Optional) Displays the MGCP-controlled endpoints.
nas	(Optional) Displays Network Access Server (NAS) information.
dump	(Optional) Display MGCP data channel data.
slot	(Optional) Slot number.
port	(Optional) Port number.
chan-number	(Optional) Channel number.
info	(Optional) Displays MGCP data channel information.
notify-entity	(Optional) Displays MGCP notify entity information.
profile [*name*]	(Optional) Displays information about all the configured MGCP profiles. • *name* --Displays information about the specified MGCP profile.
statistics	(Optional) Displays MGCP statistics regarding received and transmitted network messages.

Command Modes

User EXEC (>)
Privileged EXEC (#)

Command History

Release	Modification
12.1(1)T	This command was introduced on the Cisco AS5300.
12.1(3)T	This command was modified. Command output was updated to display additional gateway and platform information.
12.1(5)XM	This command was modified. Command output was updated to display additional gateway and platform information.
12.2(2)T	This command was implemented on the Cisco 7200 series.
12.2(2)XA	This command was modified. The **profile** keyword was added.
12.2(4)T	This command was integrated into Cisco IOS Release 12.2(4)T.

Release	Modification
12.2(2)XB	This command was modified. Command output was enhanced to display the status of MGCP system resource check (SRC) call admission control (CAC) and Service Assurance Agent (SA Agent) CAC. (See the Cisco IOS Release 12.2(2)XB document *MGCP VoIP Call Admission Control* .) The **nas dump** *slot port channel*and **nas info** keywords and arguments were added. Because the number of keywords increased, the command page for the **show mgcp** command was separated into the following command pages: • **show mgcp** • **show mgcp connection** • **show mgcp endpoint** • **show mgcp nas** • **show mgcp profile** • **show mgcp statistics**
12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T.
12.2(2)XN	This command was modified. Support for enhanced MGCP voice gateway interoperability was added to Cisco CallManager Version 3.1 for the Cisco 2600 series, Cisco 3600 series, and Cisco VG200 routers.
12.2(11)T	This command was integrated into Cisco IOS Release 12.2(11)T and Cisco CallManager Version 2.0. It was implemented on the Cisco AS5350, Cisco AS5400, Cisco AS5850, and Cisco IAD2420 series. The MGCP SGCP RSIP field was enhanced to show the status of the **mgcp sgcp disconnected notify**command.
12.2(13)T	This command was modified. Support was added for MGCP.
12.2(15)T	This command was implemented on Cisco 1751 and Cisco 1760 routers.
12.2(15)ZJ	This command was integrated into Cisco IOS Release 12.2(15)ZJ on the Cisco 26xxXM, Cisco 2691, Cisco 3640, Cisco 3640A, Cisco 3660, and Cisco 37xx routers.
12.3(2)T	This command was implemented on the Cisco 26xxXM, Cisco 2691, Cisco 3640, Cisco 3640A, Cisco 3660, and Cisco 37xx routers.
12.3(11)T	This command was modified. Command output was enhanced to display the enabled Secure Real-Time Transport Protocol (SRTP) package and enabled MGCP call-agent validation.
12.4(2)T	This command was modified. Command output was enhanced to display State Signaling Events (SSE) and Simple Packet Relay Transport (SPRT) configuration parameters.
12.4(11)T	This command was modified. The **show mgcp** command output was enhanced to display comedia-related configuration.
15.1(4)M	This command was integrated into Cisco IOS 15.1(4)M. The command output was enhanced to displays the configuration of the **tone-package keyword**in the MGCP- supported packages.

Usage Guidelines

This command provides high-level administrative information about the values configured for MGCP parameters on the router. For more specific information, use one of the optional keywords.

Use the **show mgcp** command to display SSE and SPRT parameters that have been configured to enable modem relay between IP secure telephone equipment (STE) and STE. The parameters are displayed only when the modem relay STE (mdste) package has been enabled using the **mgcp package-capability mdste-package**command.

Use the **show mgcp endpoint** command to display a list of MGCP endpoint responses when the configuring Media Gateway Control Protocol Basic Rate Interface Backhaul Signaling with Cisco CallManager feature.

The BRI endpoints are displayed in a similar manner to the way analog (Plain Old Telephone service) endpoints are displayed. The existing functions used for the analog endpoints are invoked. This display is independent of the platforms; hence the changes are required in the common code only.

This command checks for all the allocated "htsp_info_t" structures. These structures store information corresponding to all the endpoints. These structures are allocated only during system startup time. The structures are allocated for all the interfaces present, but the "vtsp_sdb_t" structure is allocated only for the first channel of the BRI port.

Since the endpoints that use the Media Gateway Control Protocol Application (MGCPAPP) as the application layer have to be displayed, the endpoints are displayed even if MGCPAPP is the only application being used by the endpoint. Because the MGCPAPP is shared across both the BRI channels and is port specific, both ports are displayed.

Examples

The following is partial sample output from the **show mgcp** command when the mdste modem relay package has been enabled:

```
Router# show mgcp
MGCP Admin State ACTIVE, Oper State ACTIVE - Cause Code NONE
MGCP call-agent: 10.7.0.200 3460 Initial protocol service is MGCP 0.1
MGCP validate call-agent source-ipaddr DISABLED
MGCP block-newcalls DISABLED
MGCP send SGCP RSIP: forced/restart/graceful/disconnected DISABLED
MGCP quarantine mode discard/step
MGCP quarantine of persistent events is ENABLED
MGCP dtmf-relay for VoIP disabled for all codec types
MGCP dtmf-relay for VoAAL2 disabled for all codec types
MGCP voip modem passthrough mode: NSE, codec: g711ulaw, redundancy: DISABLED,
MGCP voaal2 modem passthrough disabled
MGCP voip nse modem relay: Disabled
MGCP voip mdste modem relay: Enabled
        SPRT rx v14 hold time: 50 (ms), SPRT tx v14 hold count: 16,
        SPRT tx v14 hold time: 20 (ms), SPRT Retries: 12
        SSE redundancy interval: 20 (ms), SSE redundancy packet: 3,
        SSE t1 timer: 1000 (ms), SSE retries: 3
MGCP TSE payload: 100
MGCP T.38 Named Signalling Event (NSE) response timer: 200
MGCP Network (IP/AAL2) Continuity Test timer: 200
MGCP 'RTP stream loss' timer: 5
MGCP request timeout 500
MGCP maximum exponential request timeout 4000
MGCP gateway port: 2427, MGCP maximum waiting delay 20000
MGCP restart delay 0, MGCP vad DISABLED
MGCP rtrcac DISABLED
MGCP system resource check DISABLED
MGCP xpc-codec: DISABLED, MGCP persistent hookflash: DISABLED
MGCP persistent offhook: ENABLED, MGCP persistent onhook: DISABLED
MGCP piggyback msg ENABLED, MGCP endpoint offset DISABLED
```

```
MGCP simple-sdp ENABLED
MGCP undotted-notation DISABLED
MGCP codec type g711ulaw, MGCP packetization period 20
MGCP JB threshold lwm 30, MGCP JB threshold hwm 150
MGCP LAT threshold lwm 150, MGCP LAT threshold hwm 300
MGCP PL threshold lwm 1000, MGCP PL threshold hwm 10000
MGCP CL threshold lwm 1000, MGCP CL threshold hwm 10000
MGCP playout mode is adaptive 60, 4, 200 in msec
MGCP Fax Playout Buffer is 300 in msec
MGCP media (RTP) dscp: ef, MGCP signaling dscp: af31
MGCP default package: line-package
MGCP supported packages: gm-package dtmf-package mf-package trunk-package
                         line-package hs-package rtp-package script-package ms-package
                         dt-package mo-package mt-package sst-package mdr-package
                         fxr-package pre-package mdste-package srtp-package tone-package
MGCP Digit Map matching order: shortest match
SGCP Digit Map matching order: always left-to-right
MGCP VoAAL2 ignore-lco-codec DISABLED
MGCP T.38 Max Fax Rate is DEFAULT
MGCP T.38 Fax is ENABLED
MGCP T.38 Fax ECM is ENABLED
MGCP T.38 Fax NSF Override is DISABLED
MGCP T.38 Fax Low Speed Redundancy: 0
MGCP T.38 Fax High Speed Redundancy: 0
MGCP control bind :DISABLED
MGCP media bind :DISABLED
MGCP Upspeed payload type for G711ulaw: 0,  G711alaw: 8
MGCP Dynamic payload type for G.726-16K codec
MGCP Dynamic payload type for G.726-24K codec
MGCP Dynamic payload type for G.Clear codec
```

The following sample output displays the status of media source checking and the gateway role:

```
Router# show mgcp
MGCP Admin State ACTIVE, Oper State ACTIVE - Cause Code NONE
MGCP call-agent: 10.7.0.201 2497 Initial protocol service is MGCP 1.0
.
.
.
MGCP Dynamic payload type for NTE is 99
MGCP rsip-range is enabled for TGCP only.
MGCP Comedia role is PASSIVE
MGCP Comedia check media source is ENABLED
MGCP Comedia sdp force is DISABLED
MGCP Guaranteed scheduler time is DISABLED
MGCP DNS stale threshold is 30 seconds
.
.
.
```

The following is partial sample output from the **show mgcp** command when the mdste package has been disabled:

```
Router(config)# no mgcp package-capability mdste-package
Router(config)# exit
Router# show mgcp
MGCP voip mdste modem relay: Disabled
```

The table below describes the significant fields shown in the displays.

Table 103: show mgcp Field Descriptions

Field	Description
MGCP Admin State...Oper State	Administrative and operational state of the MGCP daemon. The administrative state controls the starting and the stopping of the application using the **mgcp** and **mgcp block-newcalls**commands. The operational state controls the normal MGCP operations.
MGCP call-agent	Address of the call agent specified in the **mgcp call-agent** or **call-agent** command and the protocol initiated for this session.
MGCP block-newcalls	State of the **mgcp block-newcalls** command.
MGCP send SGCP RSIP, disconnected	Setting for the **mgcp sgcp restart notify** and the **mgcp sgcp disconnected notify**commands (enabled or disabled).
MGCP quarantine mode	How the quarantine buffer is to handle Simple Gateway Control Protocol (SGCP) events.
MGCP quarantine of persistent events is	Specifies whether the SGCP persistent events are handled by the quarantine buffer.
MGCP dtmf-relay	Setting for the **mgcp dtmf-relay** command.
MGCP voip modem passthrough	Settings for mode, codec, and redundancy from the **mgcp modem passthrough mode**, **mgcp modem passthrough codec**, and **mgcp modem passthrough voip redundancy** commands.
MGCP voip mdste modem relay	Settings for the **mgcp modem relay voip sprt v14 receive playback**, **mgcp modem relay voip sprt v14 transmit maximum hold-count**, **mgcp modem relay voip sprt v14 transmit hold-time**, **mgcp modem relay voip sprt retries**, **mgcp modem relay voip sse redundancy**, and **mgcp modem relay voip sse t1** commands.
SPRT rx v14 hold time	Setting for the **mgcp modem relay voip sprt v14 receive playback hold-time** *time* command.
SPRT tx v14 hold count	Setting for the **mgcp modem relay voip sprt v14transmit maximum hold-count** *characters* command.
SPRT tx v14 hold time	Setting for the **mgcp modem relay voip sprt v14 transmit hold-time** *time*command.
SPRT Retries	Setting for the **mgcp modem relay voip sprt retries** command.
SSE redundancy interval	Setting for the **mgcp modem relay voip mode sse redundancy interval** *time* command.
SSE redundancy packet	Setting for the **mgcp modem relay voip mode sse redundancy packet**command.
SSE t1 timer	Setting for the **mgcp modem relay voip mode sse redundancy t1** command.

Field	Description
SSE retries	Setting for the **mgcp modem relay voip mode sse redundancy retries**command.
MGCP Comedia role	Location of gateway: • **ACTIVE** --inside NAT • **PASSIVE** --outside NAT
MGCP Comedia check media source	Global media IP and port address detection status (ENABLED or DISABLED).
MGCP Comedia sdp force	Configuration state of forced insertion of the direction attribute in the SDP (ENABLED or DISABLED)
MGCP TSE payload	Setting for the **mgcp tse payload** command.
MGCP Network (IP/AAL2) Continuity Test timer	Setting for the **net-cont-test** keyword in the **mgcp timer** command.
MGCP 'RTP stream loss' timer	Setting for the **receive-rtcp** keyword in the **mgcp timer** command.
MGCP request timeout	Setting for the **mgcp request timeout** command.
MGCP maximum exponential request timeout	Setting for the **mgcp request timeout max** command.
MGCP gateway port	UDP port specification for the gateway.
MGCP maximum waiting delay	Setting for the **mgcp max-waiting-delay** command.
MGCP restart delay	Setting for the **mgcp restart-delay** command.
MGCP vad	Setting for the **mgcp vad**command.
MGCP rtrcac	Specifies whether MGCP SA Agent CAC has been enabled with the **mgcp rtrcac** command.
MGCP system resource check	Specifies whether MGCP SRC CAC has been enabled with the **mgcp src-cac**command.
MGCP xpc-codec	Specifies whether the **mgcp sdp xpc-codec**command has been configured to generate the X-pc codec field for Session Description Protocol (SDP) codec negotiation in Network-Based Call Signaling (NCS) and Trunking Gateway Control Protocol (TGCP).
MGCP persistent hookflash	Specifies whether the **mgcp persistent hookflash** command has been configured to send persistent hookflash events to the call agent.
MGCP persistent offhook	Specifies whether the **mgcp persistent offhook** command has been configured to send persistent off-hook events to the call agent.

Field	Description
MGCP persistent onhook	Specifies whether the **mgcp persistent onhook**command has been configured to send persistent on-hook events to the call agent.
MGCP piggyback msg	Specifies whether the **mgcp piggyback message** command has been configured to enable piggyback messaging.
MGCP endpoint offset	Specifies whether the **mgcp endpoint offset** command has been configured to enable incrementing of the local portion of an endpoint name for NCS. The local portion contains the analog or digital voice port identifier.
MGCP simple-sdp	Specifies whether the **mgcp sdp simple**command has been configured to enable simple mode SDP operation.
MGCP undotted-notation	Specifies whether the **mgcp sdp notation undotted** command has been configured to enable undotted SDP notation for the codec string.
MGCP codec type	Setting for the **mgcp codec**command.
MGCP packetization period	The **packetization period**parameter setting for the **mgcp codec**command.
MGCP JB threshold lwm	Jitter-buffer minimum-threshold parameter setting for the **mgcp quality-threshold** command.
MGCP JB threshold hwm	Jitter-buffer maximum-threshold parameter setting for the **mgcp quality-threshold** command.
MGCP LAT threshold lwm	Latency minimum-threshold parameter setting for the **mgcp quality-threshold** command.
MGCP LAT threshold hwm	Latency maximum-threshold parameter setting for the **mgcp quality-threshold** command.
MGCP PL threshold lwm	Packet-loss minimum-threshold parameter setting for the **mgcp quality-threshold**command.
MGCP PL threshold hwm	Packet-loss maximum-threshold parameter setting for the **mgcp quality-threshold** command.
MGCP CL threshold lwm	Cell-loss minimum-threshold parameter setting for the **mgcp quality-threshold**command.
MGCP CL threshold hwm	Cell-loss maximum-threshold parameter setting for the **mgcp quality-threshold**command.
MGCP playout mode is	Jitter-buffer packet type and size.
MGCP default package	Package configured as the default package with the **mgcp default-package**command.

Field	Description
MGCP supported packages	Packages configured with the **mgcp package-capability** command to be supported on this gateway in this session. The Line Control Signaling Package (lcs-package) display is new in Cisco IOS Release 12.3(8)T.
MGCP voaal2 modem passthrough	Settings for mode, codec, and redundancy from the **mgcp modem passthrough mode**and **mgcp modem passthrough codec** commands.
MGCP T.38 Fax	Settings for the **mgcp fax t.38** command. The following values are displayed: • MGCP T.38 fax: ENABLED or DISABLED. • Error correction mode (ECM): ENABLED or DISABLED. • Nonstandard facilities (NSF) override: ENABLED or DISABLED. If enabled, the override code is displayed. • MGCP T.38 fax low-speed redundancy: the factor set on the gateway for redundancy. • MGCP T.38 fax high-speed redundancy: the factor set on the gateway for redundancy.

Related Commands

Command	Description
ccm-manager config	Supplies the local MGCP voice gateway with the IP address or logical name of the TFTP server from which to download XML configuration files and enable the download of the configuration.
debug ccm-manager	Displays debugging information about the Cisco CallManager.
debug mgcp	Enables debug traces for MGCP errors, events, media, packets, and parser.
isdn bind-l3 (interface BRI)	Configures the BRI to support MGCP and to bind ISDN Layer 3 with Cisco CallManager backhaul.
mgcp	Allocates resources for the MGCP and starts the daemon.
mgcp behavior comedia-check-media-src	Enables IP address and port detection from the first RTP packet received for the entire MGCP gateway.
mgcp behavior comedia-role	Indicates the location of the MGCP gateway.
mgcp behavior comedia-sdp-force	Forces the SDP to place the direction attribute in the SDP using the command as a reference.
mgcp package-capability mdste-package	Specifies the MGCP package capability type for a media gateway.
security password-group	Defines the passwords used by gatekeeper zones and associates them with an ID for gatekeeper-to-gatekeeper authentication.

Command	Description
show ccm-manager	Displays a list of Cisco CallManager servers and their current statuses, and availability.
show ccm-manager fallback-mgcp	Displays the status of the MGCP gateway fallback feature.
show mgcp connection	Displays information for active MGCP-controlled connections.
show mgcp endpoint	Displays information for MGCP-controlled endpoints.
show mgcp nas	Displays MGCP NAS information for data ports.
show mgcp profile	Displays values for MGCP profile-related parameters.
show mgcp statistics	Displays MGCP statistics regarding received and transmitted network messages.

show mgcp connection

To display information for active connections that are controlled by the Media Gateway Control Protocol (MGCP), use the **show mgcp connection** command inprivileged EXEC mode.

show mgcp connection

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.1(1)T	The **show mgcp** command was introduced on the Cisco AS5300.
12.1(3)T	The **show mgcp**command output was updated to display additional gateway and platform information.
12.1(5)XM	The **show mgcp**command output was updated to display additional gateway and platform information.
12.2(2)T	The **show mgcp** command was implemented on the Cisco 7200 series and was integrated into Cisco IOS Release 12.2(2)T.
12.2(2)XA	The **profile** keyword was added.
12.2(4)T	This command was integrated into Cisco IOS Release 12.2(4)T.
12.2(2)XB	Output for the **show mgcp**command was enhanced to display the status of MGCP System Resource Check (SRC) Call Admission Control (CAC) and Service Assurance Agent (SA Agent) CAC. (Refer to the Cisco IOS Release 12.2(2) XB online document *MGCP VoIP Call Admission Control* .) The **nas dump** *slot port channel* and **nas info** keywords and arguments were added. Because the number of keywords increased, the command page for the **show mgcp** command was separated into the following command pages: • **show mgcp** • **show mgcp connection** • **show mgcp endpoint** • **show mgcp nas** • **show mgcp profile** • **show mgcp statistics**
12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T. Support for the Cisco AS5300, Cisco AS5350, Cisco AS5400, and Cisco AS5850 is not included in this release.

Release	Modification
12.2(11)T	Support was added for the Cisco AS5300, Cisco AS5350, Cisco AS5400, Cisco AS5800, and Cisco AS5850.
12.3(11)T	Command output was enhanced to display the encryption suite used on the Secure Real-Time Transport Protocol (SRTP) connection.
12.4(2)T	Command output was enhanced to display the current media state.
12.4(11)T	Command output was enhanced to display the detected NAT address and port.

Examples

The following is sample output from the **show mgcp connection**command displaying a secure call for which the media state is modem relay mode:

```
Router# show mgcp connection
Endpoint  Call_ID(C) Conn_ID(I) (P)ort (M)ode (S)tate (CO)dec (E)vent[SIFL] (R)esult[EA]
(ME)dia
1. S2/DS1-2/1   C=A0000000010000100000000F5,4,3  I=0x2  P=17098,2662  M=3 S=4,4 CO=1 E=3,0,0,3
  R=0,0  ME=2
```

The following is sample output from this command showing the detected NAT address and port. The (P)ort output shows the local and advertised ports prior to detection. The (COM)Addr/Port output shows the detected media address and port (10.7.1.21:1500):

```
Router# show mgcp connection
Endpoint   Call_ID(C) Conn_ID (I) (P)ort (M)ode(S)tate(CO)dec (E)vent[SIFL] (R)esult[EA]
(COM)Addr/Port
S7/DS1-4/1 C=201597,768784,768785 I=0x5DD85 P=18258,19062 M=3 S=4,4 CO=2 E=2,0,0,2
R=0,0,0,2 COM=10.7.1.21:15000
```

The following is sample output from this command for encrypted connections:

```
Router# show mgcp connection
Endpoint       Call_ID(C) Conn_ID(I) (P)ort (M)ode (S)tate (CO)dec (E)vent[SIFL] (R)esult[EA]
 Encryption(K)
1. S1/DS1-0/1   C=2,1,2  I=0x2  P=18204,0  M=2  S=4,4 CO=1 E=0,0,0,0  R=0,0 K=1
```

The following is sample output from this command for VoIP connections:

```
Router# show mgcp connection
Endpoint   Call_ID(C) Conn_ID(I) (P)ort (M)ode (S)tate (C)odec (E)vent[SIFL] (R)esult[EA]
1. S0/DS1-0/1 C=103,23,24 I=0x8 P=16586,16634 M=3 S=4,4 C=5 E=2,0,0,2 R=0,0
2. S0/DS1-0/2 C=103,25,26 I=0x9 P=16634,16586 M=3 S=4,4 C=5 E=0,0,0,0 R=0,0
3. S0/DS1-0/3 C=101,15,16 I=0x4 P=16506,16544 M=3 S=4,4 C=5 E=2,0,0,2 R=0,0
4. S0/DS1-0/4 C=101,17,18 I=0x5 P=16544,16506 M=3 S=4,4 C=5 E=0,0,0,0 R=0,0
5. S0/DS1-0/5 C=102,19,20 I=0,6 P=16572,16600 M=3 S=4,4 C=5 E=2,0,0,2 R=0,0
6. S0/DS1-0/6 C=102,21,22 I=0x7 P=16600,16572 M=3 S=4,4 C=5 E=0,0,0,0 R=0,0
Total number of active calls 6
```

The following is sample output from this command for Voice over ATM Adaptation Layer 2 (VoAAL2) connections:

```
Router# show mgcp connection
Endpoint  Call_ID(C) Conn_ID(I)(V)cci/cid (M)ode (S)tate (C)odec (E)vent[SIFL] (R)esult[EA]
1.aaln/S1/1   C=1,11,12    I=0x2    V=2/10     M=3    S=4,4    C=1    E=3,0,0,3     R=0,0
Total number of active calls 1
```

The table below describes the significant fields shown in the displays.

Table 104: show mgcpconnection Field Descriptions

Field	Description
Endpoint	Endpoint for each call shown in the digital endpoint naming convention of slot number (S0) and digital line (DS1-0) number (1).
Call_ID(C)	MGCP call ID sent by the call agent, the internal Call Control Application Programming Interface (CCAPI) call ID for this endpoint, and the CCAPI call ID of the peer call legs. (CCAPI is an API that provides call control facilities to applications.)
(COM)Addr/Port	Detected media address and port.
Conn_ID(I)	Connection ID generated by the gateway and sent in the ACK message.
(P)ort	Ports used for this connection. The first port is the local User Datagram Protocol (UDP) port. The second port is the remote UDP port.
(V)cci/cid	Virtual channel connection identifier (VCCI) and channel identifier (CID) used for the VoAAL2 call.
(Me)dia	Media state, where: • 0--Voice • 1--Modem pass-through • 2--Modem relay
(M)ode	Call mode, where: • 0--Invalid value for mode. • 1--Gateway should only send packets. • 2--Gateway should only receive packets. • 3--Gateway should send and receive packets. • 4--Gateway should neither send nor receive packets. • 5--Gateway should place the circuit in loopback mode. • 6--Gateway should place the circuit in test mode. • 7--Gateway should use the circuit for network access for data. • 8--Gateway should place the connection in network loopback mode. • 9--Gateway should place the connection in network continuity test mode. • 10--Gateway should place the connection in conference mode. All other values are used for internal debugging.
(S)tate	Call state. The values are used for internal debugging purposes.

Field	Description
(Co)dec	Codec identifier. The values are used for internal debugging purposes.
(E)vent [SIFL]	Used for internal debugging.
(R)esult [EA]	Used for internal debugging.
Encryption(K)	Encryption suite, where: • 0--None • 1--AES_CM_128_HMAC_SHA1_32

Related Commands

Command	Description
debug mgcp	Enables debug traces for MGCP errors, events, media, packets, and parser.
mgcp	Allocates resources for the MGCP and starts the daemon.
mgcp behavior comedia-check-media-src	Enables ip address and port detection from the first rtp packet received for the entire MGCP gateway.
mgcp behavior comedia-role	Indicates the location of the MGCP gateway.
mgcp behavior comedia-sdp-force	Forces the SDP to place the direction attribute in the SDP using the command as a reference.
security password-group	Defines the passwords used by gatekeeper zones and associates them with an ID for gatekeeper-to-gatekeeper authentication.
show mgcp	Displays values for MGCP parameters.
show mgcp endpoints	Displays information for MGCP-controlled endpoints.
show mgcp nas	Displays MGCP NAS information for data ports.
show mgcp profile	Displays values for MGCP profile-related parameters.
show mgcp statistics	Displays MGCP statistics regarding received and transmitted network messages.

show mgcp endpoint

To display information for endpoints controlled by Media Gateway Control Protocol (MGCP), use the **show mgcp endpoint** command inprivileged EXEC mode.

show mgcp endpoint

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.1(1)T	The **show mgcp** command was introduced on the Cisco AS5300.
12.1(3)T	The **show mgcp**command output was updated to display additional gateway and platform information.
12.1(5)XM	The **show mgcp** command output was updated to display additional gateway and platform information.
12.2(2)T	The **show mgcp** command was implemented on the Cisco 7200 series and this command was integrated into Cisco IOS Release 12.2(2)T.
12.2(2)XA	The **profile** keyword was added to the **show mgcp** command.
12.2(4)T	This command was integrated into Cisco IOS Release 12.2(4)T.
12.2(2)XB	The output for the **show mgcp** command was enhanced to display the status of MGCP System Resource Check (SRC) Call Admission Control (CAC) and Service Assurance Agent (SA Agent) CAC. (Refer to the Cisco IOS Release 12.2(2) XB online document *MGCP VoIP Call Admission Control.*) In addition, the **nas dump** *slot port channel* and **nas info** keywords and arguments were added to the **show mgcp** command. Because the number of keywords increased, the command-reference page for the **show mgcp** command was separated into the following command-reference pages: • **show mgcp** • **show mgcp connection** • **show mgcp endpoint** • **show mgcp nas** • **show mgcp profile** • **show mgcp statistics**
12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T. Support for the Cisco AS5300, Cisco AS5350, Cisco AS5400, and Cisco AS5850 is not included in this release.

Release	Modification
12.2(11)T	This command is supported on the Cisco AS5300, Cisco AS5350, Cisco AS5400, Cisco AS5800, and Cisco AS5850 in this release.

Examples

The following is sample output from this command:

```
Router#
show mgcp endpoint
       ENDPOINT-NAME      V-PORT SIG-TYPE ADMIN
     ds1-0/1@nytnk116      0:1    fxs-gs     up
     ds1-0/2@nytnk116      0:1    fxs-gs     up
     ds1-0/3@nytnk116      0:1    fxs-gs     up
     ds1-0/4@nytnk116      0:1    fxs-gs     up
     ds1-0/5@nytnk116      0:1    fxs-gs     up
     ds1-0/6@nytnk116      0:1    fxs-gs     up
     ds1-0/7@nytnk116      0:1    fxs-gs     up
     ds1-0/8@nytnk116      0:1    fxs-gs     up
     ds1-0/9@nytnk116      0:1    fxs-gs     up
    ds1-0/10@nytnk116      0:1    fxs-gs     up
    ds1-0/11@nytnk116      0:1    fxs-gs     up
    ds1-0/12@nytnk116      0:1    fxs-gs     up
    ds1-0/13@nytnk116      0:1    fxs-gs     up
    ds1-0/14@nytnk116      0:1    fxs-gs     up
    ds1-0/15@nytnk116      0:1    fxs-gs     up
    ds1-0/16@nytnk116      0:1    fxs-gs     up
    ds1-0/17@nytnk116      0:1    fxs-gs     up
    ds1-0/18@nytnk116      0:1    fxs-gs     up
    ds1-0/19@nytnk116      0:1    fxs-gs     up
    ds1-0/20@nytnk116      0:1    fxs-gs     up
    ds1-0/21@nytnk116      0:1    fxs-gs     up
    ds1-0/22@nytnk116      0:1    fxs-gs     up
    ds1-0/23@nytnk116      0:1    fxs-gs     up
    ds1-0/24@nytnk116      0:1    fxs-gs     up
Interface T1 1
        ENDPOINT-NAME      V-PORT SIG-TYPE ADMIN
     ds1-1/1@nytnk116      1:1    e&m-imd    up
     ds1-1/2@nytnk116      1:1    e&m-imd    up
```

The table below describes significant fields shown in this output.

Table 105: show mgcp endpoint Field Descriptions

Field	Description
ENDPOINT-NAME	Name used by the call agent to identify a specific mgcp endpoint on a given gateway.
V-PORT	Voice port
SIG-TYPE	Signaling type for a given endpoint (for example, NONE for SS7 ISDN User Part (ISUP) and FXS-GS for Foreign Exchange Station (FXS) Ground Start).
ADMIN	Administrative status--Up or Down. (This field is populated only on residential gateway (RGW) platforms.

Related Commands

Command	Description
debug mgcp	Enables debug traces for MGCP errors, events, media, packets, and parser.
mgcp	Allocates resources for the MGCP and starts the daemon.
security password-group	Defines the passwords used by gatekeeper zones and associates them with an ID for gatekeeper-to-gatekeeper authentication.
show mgcp	Displays information for MGCP parameters.
show mgcp connection	Displays information for active MGCP-controlled connections.
show mgcp nas	Displays MGCP NAS information for data ports.
show mgcp profile	Displays values for MGCP profile-related parameters.
show mgcp statistics	Displays MGCP statistics regarding received and transmitted network messages.

show mgcp nas

To display Media Gateway Control Protocol (MGCP) network access server (NAS) information for data ports, use the **show mgcp nas** command in privileged EXEC mode.

show mgcp nas {**dump** *slot port channel* | **info**}

Syntax Description

dump *slot port channel*	Displays NAS information for the specified port and channel. The arguments are as follows:
	• *slot* --Chassis slot for interface card. Values are as follows:
	  • Cisco AS5350: From 0 to 3.
	  • Cisco AS5400: From 0 to 7.
	  • Cisco AS5850: From 0 to 5 and from 8 to 13. Slots 6 and 7 are reserved for the route switch controller (RSC).
	• *port* --Modem interface port. Values are as follows:
	  • Cisco AS5350: For T1/E1, from 0 to 7. For T3, from 1 to 28.
	  • Cisco AS5400: For T1/E1, from 0 to 7. For T3, from 1 to 28.
	  • Cisco AS5850: For T1/E1, from 0 to 23. For T3, from 1 to 28.
	• *channel* --T1 or E1 channel. Values for T1 are from 1 to 24. Values for E1 are from 1 to 31.

info	Displays status of NAS channels.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.1(1)T	The **show mgcp** command was introduced on the Cisco AS5300.
12.1(3)T	The **show mgcp** command output was updated to display additional gateway and platform information.
12.1(5)XM	The **show mgcp** command output was updated to display additional gateway and platform information.
12.2(2)T	The **show mgcp** command was implemented on the Cisco 7200 series and this command was integrated into Cisco IOS Release 12.2(2)T.
12.2(2)XA	The **profile** keyword was added to the **show mgcp** command.
12.2(4)T	This command was integrated into Cisco IOS Release 12.2(4)T.

Release	Modification
12.2(2)XB	The output for the **show mgcp** command was enhanced to display the status of MGCP System Resource Check (SRC) Call Admission Control (CAC) and Service Assurance Agent (SA Agent) CAC. (Refer to the Cisco IOS Release 12.2(2) XB online document *MGCP VoIP Call Admission Control.*) In addition, the **nas dump** *slot port channel* and **nas info** keywords and arguments were added to the **show mgcp** command. Because the number of keywords increased, the command-reference page for the **show mgcp** command was separated into the following command-reference pages: • **show mgcp** • **show mgcp connection** • **show mgcp endpoint** • **show mgcp nas** • **show mgcp profile** • **show mgcp statistics**
12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T. Support for the Cisco AS5300, Cisco AS5350, Cisco AS5400, and Cisco AS5850 is not included in this release.
12.2(11)T	This command is supported on the Cisco AS5300, Cisco AS5350, Cisco AS5400, Cisco AS5800, and Cisco AS5850 in this release.
12.3(7)YB	The valid values for the bearer cap field of the **show mgcp nas dump** command output were changed to include LAPB, V.120, and sync data. The Signaling field was added to the **show mgcp nas dump** command output. See the table below.
12.4(6)T	This command was integrated into Cisco IOS Release 12.4(6)T

Examples

The following is sample output from this command for an autodetected V.120 call:

```
Router# show mgcp nas dump 1 7 24
Slot 1 state=Up
Port 7 state=Up
State In Use PortCb=0x6577949C ss_id=0x0 handle=0x65C88228
Bearer Cap=V.120 call_id=1 conn_id=6577B8EC
Sig Type=Autodetect
Events req- nas/crq- req id=7 :nas/of- req id=7 :
Endpt name=S1/DS1-7/24
call_id = 1, conn_id=0x6577B8EC cgn=1000 cdn=5555
Rx packets=610  Rx bytes=73242 Tx packets 716 Tx bytes 72987
```

The table below describes the significant fields shown in the display.

Table 106: show mgcp nas dump Field Descriptions

Field	Description
Slot state	Status of specified slot.

Field	Description
Port state	Status of specified port.
State	Call status for the specified channel.
bearer cap	Bearer capability. Values are: • Modem • LAPB • V.110 • V.120 • Digital 64 • Digital 56 V.110, V.120, modem, or digital values are displayed when autodetection is not enabled and the signaling type is set to External. LAPB, V.120, and digital values are displayed if autodetection is enabled, and the signaling type is set to Autodetect.
call_id	Call identification for the currently active call, if any.
conn_id	Connection identification for the currently active call, if any.
Signaling	Call type signaling. Values are: • External--Call type is signaled by the call agent. • Autodetect--Call type is autodetected by the gateway.
Events req	List of NAS events requested, if any, and their request IDs. The request ID identifies the MGCP message from the call agent that requested the events.
Endpt name	MGCP endpoint name.

The following sample output from this command shows the state, either Idle or In Use, for each channel:

```
Router# show mgcp nas info
Number of ports configured=1
Slot 1 configured  slot state=Up  Port 7 state=Up
=====Port 7 Channel States=====
 0  Idle
 1  Idle
 2  Idle
 3  Idle
 4  Idle
 5  Idle
 6  Idle
 7  Idle
 8  Idle
 9  Idle
 10 Idle
 11 Idle
```

```
 12 Idle
 13 Idle
 14 Idle
 15 Idle
 16 Idle
 17 Idle
 18 Idle
 19 Idle
 20 Idle
 21 Idle
 22 Idle
 23 In Use
=====================================
```

Related Commands

Command	Description
debug mgcp	Enables debug traces for MGCP errors, events, media, packets, and parser.
mgcp	Allocates resources for the MGCP and starts the daemon.
security password-group	Defines the passwords used by gatekeeper zones and associates them with an ID for gatekeeper-to-gatekeeper authentication.
show mgcp	Displays information for MGCP parameters.
show mgcp connection	Displays information for active MGCP-controlled connections.
show mgcp endpoint	Displays information for MGCP-controlled endpoints.
show mgcp profile	Displays values for MGCP profile-related parameters.
show mgcp statistics	Displays MGCP statistics regarding received and transmitted network messages.

show mgcp profile

To display information for Media Gateway Control Protocol (MGCP) profiles, use the **show mgcp profile** command in privileged EXEC mode.

show mgcp profile [*profile-name*]

Syntax Description

profile -name	(Optional) Name of the MGCP profile for which information should be displayed; limited to 32 characters.

Command Default

If the optional *profile-name* argument is not used, all configured profiles are displayed.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.1(1)T	The **show mgcp** command was introduced on the Cisco AS5300.
12.1(3)T	The **show mgcp** command output was updated to display additional gateway and platform information.
12.1(5)XM	The **show mgcp** command output was updated to display additional gateway and platform information.
12.2(2)T	The **show mgcp** command was implemented on the Cisco 7200 series and this command was integrated into Cisco IOS Release 12.2(2)T.
12.2(2)XA	The **profile** keyword was added to the **show mgcp** command.
12.2(4)T	This command was integrated into Cisco IOS Release 12.2(4)T.
12.2(2)XB	Output for the **show mgcp**command was enhanced to display the status of MGCP System Resource Check (SRC) Call Admission Control (CAC) and Service Assurance Agent (SA Agent) CAC. (See the Cisco IOS Release 12.2(2)XB online document *MGCP VoIP Call Admission Control.*) In addition, the **nas dump** *slot port channel* and **nas info** keywords and arguments were added to the **show mgcp** command. Because the number of keywords increased, the command-reference page for the **show mgcp** command was separated into the following command-reference pages: • **show mgcp** • **show mgcp connection** • **show mgcp endpoint** • **show mgcp nas** • **show mgcp profile** • **show mgcp statistics**

Release	Modification
12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T. Support for the Cisco AS5300, Cisco AS5350, Cisco AS5400, and Cisco AS5850 is not included in this release.
12.2(11)T	This command is supported on the Cisco AS5300, Cisco AS5350, Cisco AS5400, Cisco AS5800, and Cisco AS5850 in this release.
12.4(4)T	Output was added to show the order in which ANI and DNIS digits are sent to the call agent.

Examples

The following is sample output for this command for the default profile:

```
Router# show mgcp profile default
MGCP Profile default
Description: None
Call-agent: none Initial protocol service is unknown
Tsmax timeout is 20 sec, Tdinit timeout is 15 sec
Tdmin timeout is 15 sec, Tdmax timeout is 600 sec
Tcrit timeout is 4 sec, Tpar timeout is 16 sec
Thist timeout is 30 sec, MWI timeout is 16 sec
Ringback tone timeout is 180 sec, Ringback tone on connection timeout is 180 sec
Network congestion tone timeout is 180 sec, Busy tone timeout is 30 sec
Dial tone timeout is 16 sec, Stutter dial tone timeout is 16 sec
Ringing tone timeout is 180 sec, Distinctive ringing tone timeout is 180 sec
Continuity1 tone timeout is 3 sec, Continuity2 tone timeout is 3 sec
Reorder tone timeout is 30 sec,  Persistent package is ms-package
Max1 DNS lookup: ENABLED, Max1 retries is 5
Max2 DNS lookup: ENABLED, Max2 retries is 7
Source Interface: NONE
T3 endpoint naming convention is T1
CAS Notification Digit order is DNIS-ANI
```

The following is sample output for this command for a profile named "example"*:*

```
Router# show mgcp profile example
MGCP Profile example
Description:None
Call-agent:10.9.57.6 5003 Initial protocol service is MGCP 1.0
Tsmax timeout is 20, Tdinit timeout is 15
Tdmin timeout is 15, Tdmax timeout is 600
Tcrit timeout is 4, Tpar timeout is 16
Thist timeout is 30, MWI timeout is 16
Ringback tone timeout is 180, Ringback tone on connection timeout is 180
Network congestion tone timeout is 180, Busy tone timeout is 30
Dial tone timeout is 16, Stutter dial tone timeout is 16
Ringing tone timeout is 180, Distinctive ringing tone timeout is 180
Continuity1 tone timeout is 3, Continuity2 tone timeout is 3
Reorder tone timeout is 30,  Persistent package is ms-package
Max1 DNS lookup:ENABLED, Max1 retries is 4
Max2 DNS lookup:ENABLED, Max2 retries is 6
Voice port:1
```

The table below describes significant fields shown in these outputs.

Table 107: show mgcp profile Field Descriptions

Field	Description
MGCP Profile	The name configured for this profile with the **mgcp profile** command.

Field	Description
Description	Description configured for this profile with the **description MGCP profile**command.
Call-agent	Domain name server (DNS) or IP address of the call agent, as configured for this profile with the **call-agent**command.
Initial protocol service	Protocol service to be used, as configured for this profile with the **call-agent** command.
Tsmax timeout	Maximum timeout value for removing messages from the retransmission queue, as configured for this profile by the **timeout tsmax** command.
Tdinit timeout	Initial waiting delay, as configured for this profile by the **timeout tdinit** command.
Tdmin timeout	Minimum timeout value for the disconnected procedure, as configured for this profile by the **timeout tdmin** command.
Tdmax timeout	Maximum timeout value for the disconnected procedure, as configured for this profile by the **timeout tdmax** command.
Tcrit timeout	Critical timeout value for the interdigit timer used in digit matching, as configured for this profile by the **timeout tcrit** command.
Tpar timeout	Partial timeout value for the interdigit timer used in digit matching, as configured for this profile by the **timeout tpar** command.
Thist timeout	Packet storage timeout value, as configured for this profile by the **timeout thist** command.
MWI timeout	Timeout value for message-waiting-indicator tone, as configured for this profile by the **timeout tone mwi** command.
Ringback tone timeout	Timeout value for ringback tone, as configured for this profile by the **timeout tone ringback** command.
Ringback tone on connection timeout	Timeout value for ringback tone on connection, as configured for this profile by the **timeout tone ringback connection** command.
Network congestion tone timeout	Timeout value for the network congestion tone, as configured for this profile by the **timeout tone network congestion** command.
Busy tone timeout	Timeout value for the busy tone, as configured for this profile by the **timeout tone busy** command.
Dial tone timeout	Timeout value for the dial tone, as configured for this profile by the **timeout tone dial** command.
Stutter dial tone timeout	Timeout value for the stutter dial tone, as configured for this profile by the **timeout tone dial stutter** command.
Ringing tone timeout	Timeout value for the ringing tone, as configured for this profile by the **timeout tone ringing** command.

Field	Description
Distinctive ringing tone timeout	Timeout value for the distinctive ringing tone, as configured for this profile by the **timeout tone ringing distinctive** command.
Continuity1 tone timeout	Timeout value for the continuity1 tone, as configured for this profile by the **timeout tone cot1** command.
Continuity2 tone timeout	Timeout value for the continuity2 tone, as configured for this profile by the **timeout tone cot2** command.
Reorder tone timeout	Timeout value for the reorder tone, as configured for this profile by the **timeout tone reorder** command.
Persistent package	Name of package configured as persistent for this profile by the **package persistent** command.
Max1 lookup	Domain name server (DNS) lookup for the call agent after the suspicion threshold is reached, as configured for this profile by the **max1 lookup** command.
Max1 retries	Number of retries to reach the call agent before a new DNS lookup is performed, as configured for this profile by the **max1 retries** command.
Max2 lookup	DNS lookup for the call agent after the disconnected threshold is reached, as configured by the **max2 lookup** command.
Max2 retries	Maximum number of retries to reach the call agent before a new DNS lookup is performed, as configured by the **max2 retries** command.
CAS Notification Digit order	Order in which ANI and DNIS digits are sent in the notify message as configured with the **notify** command.

Related Commands

Command	Description
debug mgcp	Enables debug traces for MGCP errors, events, media, packets, and parser.
mgcp	Allocates resources for the MGCP and starts the daemon.
security password-group	Defines the passwords used by the gatekeeper zones and associates them with an ID for gatekeeper-to-gatekeeper authentication.
show mgcp	Displays information for MGCP parameters.
show mgcp connection	Displays information for active MGCP-controlled connections.
show mgcp endpoint	Displays information for MGCP-controlled endpoints.
show mgcp nas	Displays MGCP NAS information for data ports.
show mgcp statistics	Displays MGCP statistics regarding received and transmitted network messages.

show mgcp srtp

To display information for active Secure Real-Time Transport Protocol (SRTP) connections that are controlled by Media Gateway Control Protocol (MGCP), use the **show mgcp srtp** command inprivileged EXEC mode.

show mgcp srtp {**summary** | **detail** [*endpoint*]}

Syntax Description

summary	Displays MGCP SRTP connections summary.

detail *endpoint*	Displays MGCP SRTP connections details.
	• The *endpoint* argument allows you to limit the display to endpoints for a specific connection. The *endpoint*argument can take the following values:
	  • Port numbers.
	  • The asterisk wildcard character*.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.3(11)T	This command was introduced.

Usage Guidelines

This command provides information about secure calls created by the MGCP application. To specify connection endpoints for display, use the **show mgcp srtp detail endpoint** command. To display valid values for the *endpoint* argument, that is, the endpoint port numbers, use the **show mgcp connection** command. Use the **show mgcp srtp detail** command to display a hashed version of the primary key and salts (encryption mechanisms) used on each connection. This display allows you to validate keys and salts for each endpoint of a call without revealing the actual primary key and salt.

Examples

The following is sample output from this command for encrypted connections:

```
Router# show mgcp srtp summary
MGCP SRTP Connection Summary
Endpoint             Conn Id    Crypto Suite
aaln/S3/SU0/0        8          AES_CM_128_HMAC_SHA1_32
aaln/S3/SU0/1        9          AES_CM_128_HMAC_SHA1_32
S3/DS1-0/1           6          AES_CM_128_HMAC_SHA1_32
S3/DS1-0/2           7          AES_CM_128_HMAC_SHA1_32
4 SRTP connections active


Router# show mgcp srtp detail
MGCP SRTP Connection Detail for Endpoint *

Definitions: CS=Crypto Suite, KS=HASHED Key/Salt, SSRC=Syncronization Source, ROC=Rollover
 Counter, KDR=Key Derivation Rate, SEQ=Sequence Number, FEC=FEC Order, MLT=Key Lifetime,
MKI=Key Index:MKI Size

Endpoint aaln/S0/SU2/1 Call ID 40294955 Conn ID 4
```

```
  Tx:CS=AES_CM_128_HMAC_SHA1_32 KS=2FFkUcBi/+XbiwKapdySC0F4nOQ= SSRC=Random ROC=0 KDR=1
SEQ=Random FEC=FEC->SRTP MLT=0x80000000 MKI=0:0
  Rx:CS=AES_CM_128_HMAC_SHA1_32 KS=XrCnoQ4ef8385GRNdTIUnFkbkN0= SSRC=Random ROC=0 KDR=1
SEQ=Random FEC=FEC->SRTP MLT=0x80000000 MKI=0:0

1 SRTP connections displayed


Router# show mgcp srtp detail S3/DS1-0/
*
show mgcp srtp detail aaln/S0/SU2/1
MGCP SRTP Connection Detail for Endpoint aaln/S0/SU2/1

Definitions: CS=Crypto Suite, KS=HASHED Key/Salt, SSRC=Syncronization Source, ROC=Rollover
 Counter, KDR=Key Derivation Rate, SEQ=Sequence Number, FEC=FEC Order, MLT=Key Lifetime,
MKI=Key Index:MKI Size

Endpoint aaln/S0/SU2/1 Call ID 40294955 Conn ID 4
  Tx:CS=AES_CM_128_HMAC_SHA1_32 KS=2FFkUcBi/+XbiwKapdySC0F4nOQ= SSRC=Random ROC=0 KDR=1
SEQ=Random FEC=FEC->SRTP MLT=0x80000000 MKI=0:0
  Rx:CS=AES_CM_128_HMAC_SHA1_32 KS=ayYP5V9d+z2L4fUNyk8E7VwOGs8= SSRC=Random ROC=0 KDR=1
SEQ=Random FEC=FEC->SRTP MLT=0x80000000 MKI=0:0

1 SRTP connections displayed
```

The table below describes the significant fields shown in the display.

Table 108: show mgcpsrtp Field Descriptions

Field	Description
Endpoint	Endpoint for each call, shown in the digital endpoint naming convention of slot number (S0) and digital line (DS1-0) number (1).
Call ID	MGCP call ID sent by the call agent.
Conn ID	Connection ID generated by the gateway and sent in the ACK message.
Crypto Suite	Identifies the cryptographic suite used on the connection.

Related Commands

Command	Description
debug mgcp	Enables debug traces for MGCP errors, events, media, packets, and parser.
mgcp	Allocates resources for the MGCP and starts the daemon.
security password-group	Defines the passwords used by gatekeeper zones and associates them with an ID for gatekeeper-to-gatekeeper authentication.
show mgcp	Displays values for MGCP parameters.
show mgcp connection	Displays information for active MGCP-controlled connections.
show mgcp endpoint	Displays information for MGCP-controlled endpoints.
show mgcp nas	Displays MGCP NAS information for data ports.

Command	Description
show mgcp profile	Displays values for MGCP profile-related parameters.

show mgcp statistics

To display Media Gateway Control Protocol (MGCP) statistics regarding received and transmitted network messages, use the **show mgcp statistics**command in privileged EXEC mode.

show mgcp statistics

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.1(1)T	The **show mgcp** command was introduced on the Cisco AS5300.
12.1(3)T	The **show mgcp** command output was updated to display additional gateway and platform information.
12.1(5)XM	The **show mgcp** command output was updated to display additional gateway and platform information.
12.2(2)T	The **show mgcp** command was implemented on the Cisco 7200 series and this command was integrated into Cisco IOS Release 12.2(2)T.
12.2(2)XA	The **profile** keyword was added to the **show mgcp** command.
12.2(4)T	This command was integrated into Cisco IOS Release 12.2(4)T.
12.2(2)XB	Output for the **show mgcp** command was enhanced to display the status of MGCP system resource check (SRC) call admission control (CAC) and Service assurance agent (SA Agent) CAC. (Refer to the Cisco IOS Release 12.2(2)XB online document *MGCP VoIP Call Admission Control.*) The **nas dump** *slot port channel* and **nas info** keywords and arguments were added to the **show mgcp** command. To simplify the command reference, the command page for the **show mgcp** command was separated into the following command pages: • **show mgcp** • **show mgcp connection** • **show mgcp endpoint** • **show mgcp nas** • **show mgcp profile** • **show mgcp statistics**
12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T. Support for the Cisco AS5300, Cisco AS5350, Cisco AS5400, and Cisco AS5850 is not included in this release.

Release	Modification
12.2(11)T	This command is supported on the Cisco AS5300, Cisco AS5350, Cisco AS5400, Cisco AS5800, and Cisco AS5850 in this release.
12.3(11)T	Output was enhanced to display dropped packets from unconfigured call agents if call-agent validation is enabled.

Examples

The following is sample output from this command for VoIP and VoAAL2 statistics:

```
Router# show mgcp statistics
UDP pkts rx 8, tx 9
Unrecognized rx pkts 0, MGCP message parsing errors 0
Duplicate MGCP ack tx 0, Invalid versions count 0
Rx packets from unknown Call Agent 0
CreateConn rx 4, successful 0, failed 0
DeleteConn rx 2, successful 2, failed 0
ModifyConn rx 4, successful 4, failed 0
DeleteConn tx 0, successful 0, failed 0
NotifyRequest rx 0, successful 4, failed 0
AuditConnection rx 0, successful 0, failed 0
AuditEndpoint rx 0, successful 0, failed 0
RestartInProgress tx 1, successful 1, failed 0
Notify tx 0, successful 0, failed 0
ACK tx 8, NACK tx 0
ACK rx 0, NACK rx 0
IP address based Call Agents statistics:
IP address 10.24.167.3, Total msg rx 8, successful 8, failed 0
```

The following is an example of the MGCP VoIP SRC CAC portion of this command output for a gateway configured with MGCP VoIP SRC CAC:

```
Router# show mgcp statistics
MGCP System Resource Check Statistics:
-------------------------------------
Total CreateConn checked by SRC :0
CreateConn accepted by SRC:0
CreateConn rejected by SRC:0
Total ModifyConn checked by SRC :0
ModifyConn accepted by SRC:0
ModifyConn rejected by SRC:0
Reason          Num. of requests rejected
------          -------------------------
cpu-5sec:       0
cpu-avg:        0
total-mem:      0
io-mem:         0
proc-mem:       0
total-calls:    0
```

The table below describes significant fields shown in this output.

Table 109: show mgcp statistics Field Descriptions

Field	Description
UDP pkts rx, tx	Number of User Datagram Protocol (UDP) packets transmitted and received from the call agent by the gateway MGCP application.

Field	Description
Unrecognized rx pkts	Number of unrecognized UDP packets received by the MGCP application.
MGCP message parsing errors	Number of MGCP messages received with parsing errors.
Duplicate MGCP ack tx	Number of duplicate MGCP acknowledgment messages transmitted to the call agents.
Invalid versions count	Number of MGCP messages received with invalid MGCP protocol versions.
Rx packets from unknown Call Agent	Number of dropped packets from unconfigured call agents.
CreateConn rx	Number of Create Connection (CRCX) messages received by the gateway, the number that were successful, and the number that failed.
DeleteConn rx	Number of Delete Connection (DLCX) messages received by the gateway, the number that were successful, and the number that failed.
DeleteConn tx	Number of DLCX messages sent from the gateway to the call agent (CA).
ModifyConn rx	Number of Modify Connection (MDCX) messages received by the gateway, the number that were successful, and the number that failed.
NotifyRequest rx	Number of Notify Request (RQNT) messages received by the gateway, the number that were successful, and the number that failed.
AuditConnection rx	Number of Audit Connection (AUCX) messages received by the gateway, the number that were successful, and the number that failed.
AuditEndpoint rx	Number of Audit Endpoint (AUEP) messages received by the gateway, the number that were successful, and the number that failed.
RestartInProgress tx	Number of Restart in Progress (RSIP) messages sent by the gateway, the number that were successful, and the number that failed.
Notify tx	Number of Notify (NTFY) messages sent by the gateway, the number that were successful, and the number that failed.
ACK tx, NACK tx	Number of Acknowledgment and Negative Acknowledgment messages sent by the gateway.
ACK rx, NACK rx	Number of Acknowledgment and Negative Acknowledgment messages received by the gateway.
IP address based Call Agents statistics: IP address, Total msg rx	IP address of the call agent, the total number of MGCP messages received from that call agent, the number of messages that were successful, and the number of messages that failed.
Total CreateConn checked by SRC	Total number of Create Connection (CRCX) messages that have been checked against the SRC component.

Field	Description
CreateConn accepted by SRC	Number of CRCX messages that have been accepted after being checked by the SRC component.
CreateConn rejected by SRC	Number of CRCX messages that have been rejected by SRC because of resource constraints.
Total ModifyConn checked by SRC	Total number of Modify Connection (MDCX) messages that have been checked against the SRC component.
ModifyConn accepted by SRC	Number of MDCX messages that have been accepted after being checked by the SRC component.
ModifyConn rejected by SRC	Number of MDCX messages that have been rejected by SRC because of resource constraints.
Reason	Specific threshold that was exceeded to cause the rejection.
Num. of requests rejected	Number of requests that have been rejected.
cpu-5sec	CPU utilization for previous 5 seconds threshold was exceeded.
cpu-avg	Average CPU utilization threshold was exceeded.
total-mem	Total memory utilization threshold was exceeded.
io-mem	I/O memory utilization threshold was exceeded.
proc-mem	Processor memory utilization threshold was exceeded.
total-calls	Total number of calls threshold was exceeded.

Related Commands

Command	Description
debug mgcp	Enables debug traces for MGCP errors, events, media, packets, and parser.
mgcp	Allocates resources for the MGCP and starts the daemon.
security password-group	Defines the passwords used by gatekeeper zones and associates them with an ID for gatekeeper-to-gatekeeper authentication.
show mgcp	Displays information for MGCP parameters.
show mgcp connection	Displays information for active MGCP-controlled connections.
show mgcp endpoint	Displays information for MGCP-controlled endpoints.
show mgcp nas	Displays MGCP NAS information for data ports.
show mgcp profile	Displays values for MGCP profile-related parameters.

show modem relay statistics

To display various statistics for modem relay, use the **show modem relay statistics** command in privileged EXEC mode.

show modem relay statistics {**all** | **phy** | **pkt** | **queue** | **sprt** | **timer** | **v14** | **v42**} [**call-identifier** *call-setup-time call-index*]

Syntax Description

all	All statistics associated with the modem-relay feature.
phy	Modem-relay physical layer statistics.
pkt	Modem-relay packetizer statistics.
queue	Modem-relay queue statistics.
sprt	Modem-relay SPRT layer statistics.
timer	Modem-relay timer statistics.
v14	Modem-relay V.14 statistics
v42	Modem-relay V.42 statistics.
call -identifier *call-setup-time*	(Optional) Value of the system UpTime when the call that is associated with this entry was started. Range is from 0 to 4294967295.
call -identifier *call-index*	(Optional) Dial-peer identification number used to distinguish between calls with the same setup time. Range is from 0 to 4294967295.

Command Default

No statistics are displayed.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.2(11)T	This command was introduced on the Cisco 2600 series, Cisco 3620, Cisco 3640, Cisco 3660, and Cisco 7200 series, and Cisco AS5300.
12.4(2)T	The **v14** keyword was added.

Usage Guidelines

Use this command to display various modem-relay call statistics, including counts of different types of packets, errors, and events, for all modem-relay calls.

Display statistics for a specific modem-relay call by using the **call-identifier** keyword and specifying the call-setup time and call index of the desired call. Obtain values for the call-setup time and call index from the SetupTime and Index fields at the start of each call record in the **show call active** command output.

Examples

The following is sample output from the **show modem relay statistics v14** command:

```
Router# show modem relay statistics v14
```

ID:11D6

V14 Layer Statistics

```
        sync_count=47 sync_loss_count=46
        min_bundle_size_rcvd_local=1 max_bundle_size_rcvd_local=20
        min_bundle_size_rcvd_remote=0 max_bundle_size_rcvd_remote=0
        info_bytes_removed_dueto_phy_rcv_q=0
        overflow_count_rcv_q=0
        info_bytes_removed_dueto_old_age_rcv_q=0
        info_bytes_discarded_bad_offset_rcv_q=0
        info_bytes_overwrite_rcv_q=0
        info_bytes_filled_rcv_q=0
        total_bytes_rcv_local=310
        min_bundle_size_send_local=0, max_bundle_size_send_local=0
        min_bundle_size_send_network=1, max_bundle_size_send_network=22
        info_bytes_removed_dueto_phy_xmit_q=0, overflow_count_xmit_q=0
        info_bytes_discarded_bad_offset_xmit_q=0
        info_bytes_overwrite_xmit_q=0
        info_bytes_filled_xmit_q=0, total_bytes_xmit_local=0
        Total Modem Relay Call Legs = 1
```

The following is sample output from this command:

```
Router# show modem relay statistics all call-identifier 43009 1
ID:3
SPRT Layer Statistics
        sprt_info_frames_rcvd=10 sprt_xid_frames_rcvd=0
        sprt_tc0_explicit_acks_rcvd=6 sprt_tc1_explicit_acks_rcvd=122
        sprt_tc2_explicit_acks_rcvd=126 sprt_destructive_brks_rcvd=0
        sprt_expedited_brks_rcvd=0
        sprt_non_expedited_brks_rcvd=0
        sprt_info_tframes_sent=9 sprt_info_tframes_resent=0
        sprt_xid_frames_sent=0 sprt_tc0_explicit_acks_sent=8
        sprt_tc1_explicit_acks_sent=129 sprt_tc2_explicit_acks_sent=132
        sprt_destructive_brks_sent=0
        sprt_expedited_brks_sent=0
        sprt_non_expedited_brks_sent=0
        sprt_info_tframes_asked_to_consumed=10
        sprt_info_tframes_consumed=10
        sprt_info_tframes_failed_to_consume=0
        sprt_info_bytes_rcvd=10 sprt_info_bytes_sent=76
        sprt_pkts_dropped_intf_busy=289 sprt_min_rexmit_timeout=500
        sprt_max_rexmit_timeout=500
Queue Statistics
        sprt_tc1_rcv_qdrops=0 sprt_tc1_xmit_qdrops=0
        sprt_tc2_rcv_qdrops=0 sprt_tc2_xmit_qdrops=0
        pktizer_out_qdrops=4 pktizer_in_qdrops=0 v42_xmit_qdrops=0
V42 Layer Statistics
        vs_chng_dueto_timeouts=0 vs_chng_dueto_rej=0
        vs_chng_dueto_rnr_resp_f1_set=0 nr_seq_exception=0
        good_rcvd_lapm_pkts=1385 discarded_rcvd_lapm_pkts=0
        rejected_rcvd_lapm_pkts=0 v42_rcvd_iframe=9
        v42_rcvd_rr=1374 v42_rcvd_rnr=0 v42_rcvd_rej=0
        v42_rcvd_srej=0 v42_rcvd_sabme=0 v42_rcvd_dm=0
        v42_rcvd_ui=0 v42_rcvd_disc=0 v42_rcvd_ua=1
        v42_rcvd_frmr=0 v42_rcvd_xid=1 v42_rcvd_test=0
        v42_rcvd_destructive_brk=0 v42_rcvd_expedited_brk=0
        v42_rcvd_non_expedited_brk=0 v42_rcvd_brkack=0
        v42_sent_iframe=10 v42_sent_rr=1464 v42_sent_rnr=0
```

```
        v42_sent_rej=0 v42_sent_srej=0 v42_sent_sabme=1
        v42_sent_dm=0 v42_sent_ui=0 v42_sent_disc=0
        v42_sent_ua=0 v42_sent_frmr=0 v42_sent_xid=1
        v42_sent_test=0 v42_sent_destructive_brk=0
        v42_sent_expedited_brk=0
        v42_sent_non_expedited_brk=0
        v42_sent_brkack=0
Physical Layer Statistics
        num_local_retrain=0 num_remote_retrain=0
        num_local_speed_shift=0 num_remote_speed_shift=0
        num_sync_loss=0
Packetizer Statistics
        frames_inprogress=5 good_crc_frames=1385
        bad_crc_frames=31 frame_aborts=124
        hdlc_sync_detects=1 hdlc_sync_loss_detects=0
        bad_frames=0
Timer Statistics
        xid_timer_cnt=0 sabme_timer_cnt=0 ack_timer_cnt=0
        chkpnt_timer_cnt=1333
```

The following is sample output from this command:

```
Router# show modem relay statistics all
ID:3
SPRT Layer Statistics
        sprt_info_frames_rcvd=10 sprt_xid_frames_rcvd=0
        sprt_tc0_explicit_acks_rcvd=6 sprt_tc1_explicit_acks_rcvd=155
        sprt_tc2_explicit_acks_rcvd=158 sprt_destructive_brks_rcvd=0
        sprt_expedited_brks_rcvd=0
        sprt_non_expedited_brks_rcvd=0
        sprt_info_tframes_sent=9 sprt_info_tframes_resent=0
        sprt_xid_frames_sent=0 sprt_tc0_explicit_acks_sent=8
        sprt_tc1_explicit_acks_sent=161 sprt_tc2_explicit_acks_sent=165
        sprt_destructive_brks_sent=0
        sprt_expedited_brks_sent=0
        sprt_non_expedited_brks_sent=0
        sprt_info_tframes_asked_to_consumed=10
        sprt_info_tframes_consumed=10
        sprt_info_tframes_failed_to_consume=0
        sprt_info_bytes_rcvd=10 sprt_info_bytes_sent=76
        sprt_pkts_dropped_intf_busy=357 sprt_min_rexmit_timeout=500
        sprt_max_rexmit_timeout=500
Queue Statistics
        sprt_tc1_rcv_qdrops=0 sprt_tc1_xmit_qdrops=0
        sprt_tc2_rcv_qdrops=0 sprt_tc2_xmit_qdrops=0
        pktizer_out_qdrops=4 pktizer_in_qdrops=0 v42_xmit_qdrops=0
V42 Layer Statistics
        vs_chng_dueto_timeouts=0 vs_chng_dueto_rej=0
        vs_chng_dueto_rnr_resp_f1_set=0 nr_seq_exception=0
        good_rcvd_lapm_pkts=1910 discarded_rcvd_lapm_pkts=0
        rejected_rcvd_lapm_pkts=0 v42_rcvd_iframe=9
        v42_rcvd_rr=1899 v42_rcvd_rnr=0 v42_rcvd_rej=0
        v42_rcvd_srej=0 v42_rcvd_sabme=0 v42_rcvd_dm=0
        v42_rcvd_ui=0 v42_rcvd_disc=0 v42_rcvd_ua=1
        v42_rcvd_frmr=0 v42_rcvd_xid=1 v42_rcvd_test=0
        v42_rcvd_destructive_brk=0 v42_rcvd_expedited_brk=0
        v42_rcvd_non_expedited_brk=0 v42_rcvd_brkack=0
        v42_sent_iframe=10 v42_sent_rr=1988 v42_sent_rnr=0
        v42_sent_rej=0 v42_sent_srej=0 v42_sent_sabme=1
        v42_sent_dm=0 v42_sent_ui=0 v42_sent_disc=0
        v42_sent_ua=0 v42_sent_frmr=0 v42_sent_xid=1
        v42_sent_test=0 v42_sent_destructive_brk=0
        v42_sent_expedited_brk=0
        v42_sent_non_expedited_brk=0
```

```
        v42_sent_brkack=0
Physical Layer Statistics
        num_local_retrain=0 num_remote_retrain=0
        num_local_speed_shift=0 num_remote_speed_shift=0
        num_sync_loss=0
Packetizer Statistics
        frames_inprogress=5 good_crc_frames=1910
        bad_crc_frames=31 frame_aborts=124
        hdlc_sync_detects=1 hdlc_sync_loss_detects=0
        bad_frames=0
Timer Statistics
        xid_timer_cnt=0 sabme_timer_cnt=0 ack_timer_cnt=0
        chkpnt_timer_cnt=1809
        Total Modem Relay Call Legs = 1
```

The following is sample output from this command:

```
Router# show modem relay statistics sprt
ID:3
SPRT Layer Statistics
        sprt_info_frames_rcvd=10 sprt_xid_frames_rcvd=0
        sprt_tc0_explicit_acks_rcvd=6 sprt_tc1_explicit_acks_rcvd=177
        sprt_tc2_explicit_acks_rcvd=180 sprt_destructive_brks_rcvd=0
        sprt_expedited_brks_rcvd=0
        sprt_non_expedited_brks_rcvd=0
        sprt_info_tframes_sent=9 sprt_info_tframes_resent=0
        sprt_xid_frames_sent=0 sprt_tc0_explicit_acks_sent=8
        sprt_tc1_explicit_acks_sent=183 sprt_tc2_explicit_acks_sent=187
        sprt_destructive_brks_sent=0
        sprt_expedited_brks_sent=0
        sprt_non_expedited_brks_sent=0
        sprt_info_tframes_asked_to_consumed=10
        sprt_info_tframes_consumed=10
        sprt_info_tframes_failed_to_consume=0
        sprt_info_bytes_rcvd=10 sprt_info_bytes_sent=76
        sprt_pkts_dropped_intf_busy=403 sprt_min_rexmit_timeout=500
        sprt_max_rexmit_timeout=500
        Total Modem Relay Call Legs = 1
```

The following is sample output from this command:

```
Router# show modem relay statistics queue
ID:3
Queue Statistics
        sprt_tc1_rcv_qdrops=0 sprt_tc1_xmit_qdrops=0
        sprt_tc2_rcv_qdrops=0 sprt_tc2_xmit_qdrops=0
        pktizer_out_qdrops=4 pktizer_in_qdrops=0 v42_xmit_qdrops=0
        Total Modem Relay Call Legs = 1
```

The following is sample output from this command:

```
Router# show modem relay statistics v42
ID:3
V42 Layer Statistics
        vs_chng_dueto_timeouts=0 vs_chng_dueto_rej=0
        vs_chng_dueto_rnr_resp_f1_set=0 nr_seq_exception=0
        good_rcvd_lapm_pkts=2442 discarded_rcvd_lapm_pkts=0
        rejected_rcvd_lapm_pkts=0 v42_rcvd_iframe=9
        v42_rcvd_rr=2431 v42_rcvd_rnr=0 v42_rcvd_rej=0
        v42_rcvd_srej=0 v42_rcvd_sabme=0 v42_rcvd_dm=0
        v42_rcvd_ui=0 v42_rcvd_disc=0 v42_rcvd_ua=1
        v42_rcvd_frmr=0 v42_rcvd_xid=1 v42_rcvd_test=0
        v42_rcvd_destructive_brk=0 v42_rcvd_expedited_brk=0
```

```
        v42_rcvd_non_expedited_brk=0 v42_rcvd_brkack=0
        v42_sent_iframe=10 v42_sent_rr=2539 v42_sent_rnr=0
        v42_sent_rej=0 v42_sent_srej=0 v42_sent_sabme=1
        v42_sent_dm=0 v42_sent_ui=0 v42_sent_disc=0
        v42_sent_ua=0 v42_sent_frmr=0 v42_sent_xid=1
        v42_sent_test=0 v42_sent_destructive_brk=0
        v42_sent_expedited_brk=0
        v42_sent_non_expedited_brk=0
        v42_sent_brkack=0
        Total Modem Relay Call Legs = 1
```

The following is sample output from this command:

```
Router# show modem relay statistics phy
ID:3
Physical Layer Statistics
        num_local_retrain=0 num_remote_retrain=0
        num_local_speed_shift=0 num_remote_speed_shift=0
        num_sync_loss=0
        Total Modem Relay Call Legs = 1
```

The following is sample output from this command:

```
Router# show modem relay stat pkt
ID:3
Packetizer Statistics
        frames_inprogress=5 good_crc_frames=2573
        bad_crc_frames=61 frame_aborts=150
        hdlc_sync_detects=1 hdlc_sync_loss_detects=0
        bad_frames=0
        Total Modem Relay Call Legs = 1
```

The following is sample output from this command:

```
Router# show modem relay stat timer
ID:3
Timer Statistics
        xid_timer_cnt=0 sabme_timer_cnt=0 ack_timer_cnt=0
        chkpnt_timer_cnt=2750
        Total Modem Relay Call Legs = 1
```

Related Commands

Command	Description
debug voip ccapi inout	Traces the execution path through the call control API.
debug vtsp all	Displays all VTSP debugging except statistics, tone, and event.
show call active	Displays active call information for voice calls or fax transmissions in progress.
show call active voice	Displays current call information for a call in progress.
show modems	Displays all modem configurations.



show mrcp client session active through show sip dhcp

- show monitor event-trace voip ccsip (EXEC), on page 571
- show mrcp client session active, on page 588
- show mrcp client session history, on page 591
- show mrcp client statistics hostname, on page 595
- show mwi relay clients, on page 597
- show nextport, on page 598
- show nextport vpd, on page 604
- show num-exp, on page 606
- show piafs status, on page 608
- show platform hardware qfp active feature sbc fork global, on page 610
- show platform hardware qfp active feature sbc fork session, on page 612
- show pots csm, on page 615
- show pots status, on page 616
- show pots volume, on page 620
- show presence global, on page 621
- show presence subscription, on page 623
- show proxy h323 calls, on page 627
- show proxy h323 detail-call, on page 628
- show proxy h323 status, on page 633
- show raw, on page 634
- show rawmsg, on page 636
- show rlm group statistics, on page 638
- show rlm group status, on page 641
- show rlm group timer, on page 643
- show rpms-proc counters, on page 645
- show running-config dial-peer, on page 647
- show rtpspi, on page 649
- show rtsp client session, on page 651
- show rudpv0 failures, on page 654
- show rudpv0 statistics, on page 656
- show rudpv1, on page 658

- show sccp, on page 661
- show sccp ccm group, on page 668
- show sccp connections details, on page 670
- show sccp connections internal, on page 671
- show sccp connections rsvp, on page 672
- show sccp connections summary, on page 674
- show sccp server statistics, on page 676
- show sdspfarm, on page 677
- show settlement, on page 683
- show sgcp connection, on page 685
- show sgcp endpoint, on page 687
- show sgcp statistics, on page 688
- show shared-line, on page 690
- show sip dhcp, on page 692

show monitor event-trace voip ccsip (EXEC)

To display the captured Voice over IP (VoIP) Call-Control Session Initiation Protocol (CCSIP) event-traces on console, use the **show monitor event-trace voip ccsip** command in user EXEC or privileged EXEC mode.

show monitor event-trace voip ccsip {**api** | **fsm** | **global** | **history** | **merged** | **misc** | **msg** | **summary**} [**filter** {**call-id** | **called-num** | **calling-num** | **sip-call-id**} *filter*] {**all** | **back** *duration* | **clock** *time* | **from-boot** *seconds* | **latest**}

Syntax Description

api	Displays information about event tracing for VOIP CCSIP API events.
fsm	Displays information about event tracing for Finite State Machine (FSM) and Communicating Nested FSM (CNFSM) events.
global	Displays information about event tracing for global events.
history	Displays information about all completed calls.
merged	Displays information about merged events.
misc	Displays information about miscellaneous events.
msg	Displays information about event tracing message events.
summary	Displays a summary of all captured information.
filter	(Optional) Filters information to be displayed based on the selected filter options.
call-id *filter*	Displays information related to the specified call ID.
called-num *filter*	Displays information related to the specified called number.
calling-num *filter*	Displays information related to the specified calling number.
sip-call-id *filter*	Displays information related to the specified SIP call-id.
all	Displays all event trace information in the current buffer.
back *duration*	Displays all event trace information from the current time going backwards for the duration specified.

clock *time*	Displays information from the specified time until the current time.
from-boot *seconds*	Displays information from this many seconds after boot.
latest	Displays the latest trace events since the last display.

Command Modes

User EXEC (>)

Privileged EXEC (#)

Command History

Release	Modification
15.3(3)M	This command was introduced.

Usage Guidelines

Use the **monitor event-trace voip ccsip** command to control what, when, and how event trace data is collected. Use this command after you have configured the event trace functionality on the networking device using the **monitor event-trace voip ccsip** command in global configuration mode.

Use the **show monitor event-trace voip ccsip** command to display event traces for the configured events.

Use the **filter** keyword to limit traces for specific SIP based parameters, this ensures that only relevant traces are displayed on the console.

Example

The following example shows how to display a summary of statistics for active call traces:

```
Device# show monitor event-trace voip ccsip summary
--------Cover buff----------
        buffer-id = 1   ccCallId = 1    PeerCallId = 2
        Called-Number = 22222   Calling-Number = 11111  Sip-Call-Id = 1-5671@9.40.1.22
sip_msgs: Enabled.. Total Traces logged = 8
sip_fsm: Enabled.. Total Traces logged = 22
sip_apis: Enabled.. Total Traces logged = 15
sip_misc: Enabled.. Total Traces logged = 4

--------Cover buff----------
        buffer-id = 2   ccCallId = 2    PeerCallId = 1
        Called-Number = 22222   Calling-Number = 11111  Sip-Call-Id =
7155B639-FFFFFFFFE25011E2-FFFFFFFF80088694-20A3250E@9.40.1.30
sip_msgs: Enabled.. Total Traces logged = 7
sip_fsm: Enabled.. Total Traces logged = 26
sip_apis: Enabled.. Total Traces logged = 19
sip_misc: Enabled.. Total Traces logged = 3
```

The following example shows how to display information about all miscellaneous event traces:

```
Device# show monitor event-trace voip ccsip misc all
--------Cover buff----------
        buffer-id = 1   ccCallId = 1    PeerCallId = 2
        Called-Number = 22222   Calling-Number = 11111  Sip-Call-Id = 1-5671@9.40.1.22
sip_msgs: Enabled.. Total Traces logged = 8
sip_fsm: Enabled.. Total Traces logged = 22
```

```
sip_apis: Enabled.. Total Traces logged = 15
sip_misc: Enabled.. Total Traces logged = 4
-------------------------------
*Jul  2 13:16:30.118: Inbound dial-peer matched : tag = 11111
*Jul  2 13:16:30.119: Media Stream Index = 1, Media Stream Type = voice-only Stream State
= STREAM_ADDING
        Negotiated Codec = g711ulaw Negotiated DTMF Type = inband-voice
*Jul  2 13:16:30.120: Media Stream Index = 1, Media Stream Type = voice-only Stream State
= STREAM_ADDING
        Negotiated Codec = g711ulaw Negotiated DTMF Type = inband-voice
*Jul  2 13:16:30.131: Media Stream Index = 1, Media Stream Type = voice-only Stream State
= STREAM_ADDING
        Negotiated Codec = g711ulaw Negotiated DTMF Type = inband-voice
--------Cover buff----------
        buffer-id = 2   ccCallId = 2    PeerCallId = 1
        Called-Number = 22222   Calling-Number = 11111  Sip-Call-Id =
7155B639-FFFFFFFFE25011E2-FFFFFFFF80088694-20A3250E@9.40.1.30
sip_msgs: Enabled.. Total Traces logged = 7
sip_fsm: Enabled.. Total Traces logged = 26
sip_apis: Enabled.. Total Traces logged = 19
sip_misc: Enabled.. Total Traces logged = 3
-------------------------------
*Jul  2 13:16:30.122: Outbound dial-peer matched : tag = 22222
*Jul  2 13:16:30.123: Media Stream Index = 1, Media Stream Type = voice-only Stream State
= STREAM_ADDING
        Negotiated Codec = No Codec    Negotiated DTMF Type = inband-voice
*Jul  2 13:16:30.129: Media Stream Index = 1, Media Stream Type = voice-only Stream State
= STREAM_ADDING
        Negotiated Codec = g711ulaw Negotiated DTMF Type = inband-voice
```

The following example displays the captured event traces for Finite State Machine (FSM) and Communicating Nested FSM (CNFSM) events:

```
Device# show monitor event-trace voip ccsip fsm all
--------Cover buff----------
        buffer-id = 1   ccCallId = 1    PeerCallId = 2
        Called-Number = 22222   Calling-Number = 11111  Sip-Call-Id = 1-5671@9.40.1.22
sip_msgs: Enabled.. Total Traces logged = 8
sip_fsm: Enabled.. Total Traces logged = 22
sip_apis: Enabled.. Total Traces logged = 15
sip_misc: Enabled.. Total Traces logged = 4
-------------------------------
*Jul  2 13:16:30.116: FSM TYPE = SIP STATE TRANS FSM Current State = STATE_NONE Next State
 = STATE_IDLE Current Substate = STATE_NONE Next Substate = STATE_IDLE
*Jul  2 13:16:30.118: CNFSM TYPE = SIP Offer-Answer CNFSM, Event = E_SIP_INVITE_SDP_RCVD,
     Current State = S_SIP_EARLY_DIALOG_IDLE,    Next State = S_SIP_EARLY_DIALOG_OFFER_RCVD
*Jul  2 13:16:30.118: CNFSM TYPE = SIP IWF CNFSM, Event = E_SIP_IWF_EV_RCVD_SDP,
Current State = S_SIP_IWF_SDP_IDLE, Next State = S_SIP_IWF_SDP_RCVD_AWAIT_PEER_EVENT
*Jul  2 13:16:30.119: FSM TYPE = SIP STATE TRANS FSM Current State = STATE_IDLE Next State
 = STATE_RECD_INVITE Current Substate = STATE_IDLE Next Substate = STATE_RECD_INVITE
*Jul  2 13:16:30.121: CNFSM TYPE = SIP IWF CNFSM, Event = E_SIP_IWF_EV_SET_MODE,
Current State = CNFSM_CONTAINER_STATE,      Next State = CNFSM_NO_STATE_CHANGE
*Jul  2 13:16:30.122:  FSM TYPE = SIP Event-state FSM, Event = SIPSPI_EV_CC_CALL_PROCEEDING
     Current State = STATE_RECD_INVITE
*Jul  2 13:16:30.122: CNFSM TYPE = SIP Media Service CNFSM, Event =
E_IPIP_MEDIA_SERV_EV_XCODER_RESET_STREAM,   Current State = CNFSM_CONTAINER_STATE,
Next State = S_IPIP_MEDIA_SERV_STATE_IDLE
*Jul  2 13:16:30.127:  FSM TYPE = SIP Event-state FSM, Event = SIPSPI_EV_CC_CALL_ALERTING
      Current State = STATE_RECD_INVITE
*Jul  2 13:16:30.127: FSM TYPE = SIP STATE TRANS FSM Current State = STATE_RECD_INVITE Next
 State = STATE_SENT_ALERTING Current Substate = STATE_RECD_INVITE Next Substate =
STATE_SENT_ALERTING
```

```
*Jul  2 13:16:30.128: CNFSM TYPE = SIP IWF CNFSM, Event = E_SIP_IWF_EV_PEER_CAPS,
Current State = CNFSM_CONTAINER_STATE,      Next State = CNFSM_NO_STATE_CHANGE
*Jul  2 13:16:30.130: CNFSM TYPE = SIP IWF CNFSM, Event =
E_SIP_IWF_EV_PEER_MULTIMEDIA_CHANNEL_ACK,     Current State =
S_SIP_IWF_SDP_RCVD_AWAIT_PEER_EVENT,        Next State = CNFSM_NO_STATE_CHANGE
*Jul  2 13:16:30.130: CNFSM TYPE = SIP Media Service CNFSM, Event =
E_IPIP_MEDIA_SERV_EV_PEER_CHNL_ACK, Current State = S_IPIP_MEDIA_SERV_STATE_IDLE,
Next State = CNFSM_NO_STATE_CHANGE
*Jul  2 13:16:30.139: CNFSM TYPE = SIP IWF CNFSM, Event = E_SIP_IWF_EV_CALL_CONNECT,
Current State = CNFSM_CONTAINER_STATE,      Next State = CNFSM_NO_STATE_CHANGE
*Jul  2 13:16:30.139:  FSM TYPE = SIP Event-state FSM, Event = SIPSPI_EV_CC_CALL_CONNECT
      Current State = STATE_SENT_ALERTING
*Jul  2 13:16:30.139: CNFSM TYPE = SIP Offer-Answer CNFSM, Event = E_SIP_INVITE_RESP_SDP_SENT,
  Current State = S_SIP_EARLY_DIALOG_OFFER_RCVD,      Next State =
S_SIP_EARLY_DIALOG_OFFER_ANSWER_COMPLETE
*Jul  2 13:16:30.139: CNFSM TYPE = SIP IWF CNFSM, Event = E_SIP_IWF_EV_SENT_SDP,
Current State = S_SIP_IWF_SDP_RCVD_AWAIT_PEER_EVENT,        Next State = S_SIP_IWF_SDP_DONE
*Jul  2 13:16:30.141: FSM TYPE = SIP STATE TRANS FSM Current State = STATE_SENT_ALERTING
Next State = STATE_SENT_SUCCESS Current Substate = STATE_SENT_ALERTING Next Substate =
STATE_SENT_SUCCESS
*Jul  2 13:16:30.146:  FSM TYPE = SIP Event-state FSM, Event = SIPSPI_EV_NEW_MESSAGE
Current State = STATE_SENT_SUCCESS
*Jul  2 13:16:30.146: FSM TYPE = SIP STATE TRANS FSM Current State = STATE_SENT_SUCCESS
Next State = STATE_ACTIVE Current Substate = STATE_SENT_SUCCESS Next Substate = STATE_ACTIVE
*Jul  2 13:16:30.146: CNFSM TYPE = SIP Offer-Answer CNFSM, Event = E_SIP_DIALOG_ESTD,
Current State = S_SIP_EARLY_DIALOG_OFFER_ANSWER_COMPLETE,   Next State = S_SIP_MID_DIALOG_IDLE
*Jul  2 13:16:30.146: CNFSM TYPE = SIP IWF CNFSM, Event = E_SIP_IWF_EV_CALL_ACTIVE,
Current State = CNFSM_CONTAINER_STATE,      Next State = CNFSM_NO_STATE_CHANGE
*Jul  2 13:16:30.147: CNFSM TYPE = SIP Media Service CNFSM, Event =
E_IPIP_MEDIA_SERV_EV_CALL_ACTIVE,   Current State = CNFSM_CONTAINER_STATE,      Next State
 = CNFSM_NO_STATE_CHANGE
--------Cover buff-----------
        buffer-id = 2   ccCallId = 2    PeerCallId = 1
        Called-Number = 22222   Calling-Number = 11111  Sip-Call-Id =
7155B639-FFFFFFFFE25011E2-FFFFFFFF80088694-20A3250E@9.40.1.30
sip_msgs: Enabled.. Total Traces logged = 7
sip_fsm: Enabled.. Total Traces logged = 26
sip_apis: Enabled.. Total Traces logged = 19
sip_misc: Enabled.. Total Traces logged = 3
-------------------------------
*Jul  2 13:16:30.121: FSM TYPE = SIP STATE TRANS FSM Current State = STATE_NONE Next State
 = STATE_IDLE Current Substate = STATE_NONE Next Substate = STATE_IDLE
*Jul  2 13:16:30.121: CNFSM TYPE = SIP IWF CNFSM, Event = E_SIP_IWF_EV_SET_MODE,
Current State = CNFSM_CONTAINER_STATE,      Next State = CNFSM_NO_STATE_CHANGE
*Jul  2 13:16:30.121: CNFSM TYPE = SIP IWF CNFSM, Event = E_SIP_IWF_EV_PRE_SETUP,
Current State = S_SIP_IWF_SDP_IDLE, Next State = CNFSM_NO_STATE_CHANGE
*Jul  2 13:16:30.122: CNFSM TYPE = SIP IWF CNFSM, Event =
E_SIP_IWF_EV_PEER_MULTIMEDIA_CHANNEL_IND,     Current State = S_SIP_IWF_SDP_IDLE,
Next State = CNFSM_NO_STATE_CHANGE
*Jul  2 13:16:30.122: CNFSM TYPE = SIP Media Service CNFSM, Event =
E_IPIP_MEDIA_SERV_EV_PEER_CHNL_IND, Current State = S_IPIP_MEDIA_SERV_STATE_IDLE,
Next State = S_IPIP_MEDIA_SERV_STATE_INIT_XCODER_RESERVED
*Jul  2 13:16:30.122: CNFSM TYPE = SIP IWF CNFSM, Event = E_SIP_IWF_EV_CONTINUE_PRE_SETUP,
      Current State = S_SIP_IWF_SDP_IDLE,         Next State = CNFSM_NO_STATE_CHANGE
*Jul  2 13:16:30.123: CNFSM TYPE = SIP Media Service CNFSM, Event =
E_IPIP_MEDIA_SERV_EV_XCODER_RESET_STREAM,   Current State = CNFSM_CONTAINER_STATE,
Next State = S_IPIP_MEDIA_SERV_STATE_IDLE
*Jul  2 13:16:30.123: CNFSM TYPE = SIP IWF CNFSM, Event = E_SIP_IWF_EV_INIT_CALL_SETUP,
Current State = S_SIP_IWF_SDP_IDLE, Next State = CNFSM_NO_STATE_CHANGE
*Jul  2 13:16:30.123:  FSM TYPE = SIP Event-state FSM, Event = SIPSPI_EV_CC_CALL_SETUP
      Current State = STATE_IDLE
*Jul  2 13:16:30.124: CNFSM TYPE = SIP Offer-Answer CNFSM, Event = E_SIP_INVITE_SDP_SENT,
     Current State = S_SIP_EARLY_DIALOG_IDLE,    Next State = S_SIP_EARLY_DIALOG_OFFER_SENT
*Jul  2 13:16:30.124: CNFSM TYPE = SIP IWF CNFSM, Event = E_SIP_IWF_EV_SENT_SDP,
```

```
Current State = S_SIP_IWF_SDP_IDLE, Next State = S_SIP_IWF_SDP_SENT_AWAIT_SDP
*Jul  2 13:16:30.125: FSM TYPE = SIP STATE TRANS FSM Current State = STATE_IDLE Next State
 = STATE_SENT_INVITE Current Substate = STATE_IDLE Next Substate = STATE_SENT_INVITE
*Jul  2 13:16:30.127:  FSM TYPE = SIP Event-state FSM, Event = SIPSPI_EV_NEW_MESSAGE
Current State = STATE_SENT_INVITE
*Jul  2 13:16:30.127: FSM TYPE = SIP STATE TRANS FSM Current State = STATE_SENT_INVITE Next
 State = STATE_RECD_PROCEEDING Current Substate = STATE_SENT_INVITE Next Substate =
STATE_RECD_PROCEEDING
*Jul  2 13:16:30.128:  FSM TYPE = SIP Event-state FSM, Event = SIPSPI_EV_NEW_MESSAGE
Current State = STATE_RECD_PROCEEDING
*Jul  2 13:16:30.128: CNFSM TYPE = SIP Offer-Answer CNFSM, Event = E_SIP_INVITE_RESP_SDP_RCVD,
  Current State = S_SIP_EARLY_DIALOG_OFFER_SENT,      Next State =
S_SIP_EARLY_DIALOG_OFFER_ANSWER_COMPLETE
*Jul  2 13:16:30.128: CNFSM TYPE = SIP IWF CNFSM, Event = E_SIP_IWF_EV_RCVD_SDP,
Current State = S_SIP_IWF_SDP_SENT_AWAIT_SDP,       Next State = S_SIP_IWF_SDP_DONE
*Jul  2 13:16:30.129: FSM TYPE = SIP STATE TRANS FSM Current State = STATE_RECD_PROCEEDING
 Next State = STATE_RECD_PROCEEDING Current Substate = STATE_RECD_PROCEEDING Next Substate
 = STATE_RECD_PROCEEDING
*Jul  2 13:16:30.129: FSM TYPE = SIP STATE TRANS FSM Current State = STATE_RECD_PROCEEDING
 Next State = SIP_STATE_RECD_SUCCESS Current Substate = STATE_RECD_PROCEEDING Next Substate
 = SIP_STATE_RECD_SUCCESS
*Jul  2 13:16:30.129: CNFSM TYPE = SIP Offer-Answer CNFSM, Event = E_SIP_DIALOG_ESTD,
Current State = S_SIP_EARLY_DIALOG_OFFER_ANSWER_COMPLETE,   Next State = S_SIP_MID_DIALOG_IDLE
*Jul  2 13:16:30.129: CNFSM TYPE = SIP IWF CNFSM, Event = E_SIP_IWF_EV_CALL_ACTIVE,
Current State = CNFSM_CONTAINER_STATE,      Next State = CNFSM_NO_STATE_CHANGE
*Jul  2 13:16:30.129: FSM TYPE = SIP STATE TRANS FSM Current State = SIP_STATE_RECD_SUCCESS
 Next State = STATE_ACTIVE Current Substate = SIP_STATE_RECD_SUCCESS Next Substate =
STATE_ACTIVE
*Jul  2 13:16:30.129: CNFSM TYPE = SIP IWF CNFSM, Event = E_SIP_IWF_EV_UPDATE_STREAM_CONTEXT,
   Current State = S_SIP_IWF_SDP_DONE,         Next State = CNFSM_NO_STATE_CHANGE
*Jul  2 13:16:30.130: CNFSM TYPE = SIP IWF CNFSM, Event = E_SIP_IWF_EV_PEER_CAPS_ACK,,
Current State = CNFSM_CONTAINER_STATE,      Next State = CNFSM_NO_STATE_CHANGE
*Jul  2 13:16:30.130: CNFSM TYPE = SIP IWF CNFSM, Event = E_SIP_IWF_EV_PEER_CAPS_ACK,,
Current State = CNFSM_CONTAINER_STATE,      Next State = CNFSM_NO_STATE_CHANGE
*Jul  2 13:16:30.130: CNFSM TYPE = SIP Media Service CNFSM, Event =
E_IPIP_MEDIA_SERV_EV_CALL_ACTIVE,   Current State = CNFSM_CONTAINER_STATE,      Next State
 = CNFSM_NO_STATE_CHANGE
```

The following example shows how to display information about all API event traces:

```
Device# show monitor event-trace voip ccsip api all
--------Cover buff----------
        buffer-id = 1   ccCallId = 1    PeerCallId = 2
        Called-Number = 22222   Calling-Number = 11111  Sip-Call-Id = 1-5671@9.40.1.22
sip_msgs: Enabled.. Total Traces logged = 8
sip_fsm: Enabled.. Total Traces logged = 22
sip_apis: Enabled.. Total Traces logged = 15
sip_misc: Enabled.. Total Traces logged = 4
--------------------------------
*Jul  2 13:16:30.119: API Name = cc_api_update_interface_cac_resource Ret_code= 0
*Jul  2 13:16:30.119: API Name = voip_rtp_allocate_port Port = 16384
*Jul  2 13:16:30.120: API Name = cc_api_call_setup_ind_with_callID Ret_code= 0
*Jul  2 13:16:30.123: API Name = voip_rtp_create_session Ret_code= 0
*Jul  2 13:16:30.123: API Name = voip_rtp_set_non_rtp_call Ret_code= 0
*Jul  2 13:16:30.123: API Name = voip_rtp_update_callinfo Ret_code= 0
*Jul  2 13:16:30.129: API Name = cc_api_caps_ack Ret_code= 0
*Jul  2 13:16:30.130: API Name = cc_api_caps_ack Ret_code= 0
*Jul  2 13:16:30.131: API Name = voip_rtp_update_callinfo Ret_code= 0
*Jul  2 13:16:30.131: API Name = cc_api_call_mode_update_ind Ret_code= 0
*Jul  2 13:16:30.132: API Name = voip_rtp_update_callinfo Ret_code= 0
*Jul  2 13:16:30.132: API Name = voip_rtp_set_non_rtp_call Ret_code= 0
*Jul  2 13:16:30.132: API Name = voip_rtp_update_callinfo Ret_code= 0
*Jul  2 13:16:30.132: API Name = cc_api_bridge_done Ret_code= 0
*Jul  2 13:16:30.132: API Name = ccsip_bridge Ret_code= 0
```

```
--------Cover buff----------
        buffer-id = 2   ccCallId = 2    PeerCallId = 1
        Called-Number = 22222   Calling-Number = 11111  Sip-Call-Id =
7155B639-FFFFFFFFE25011E2-FFFFFFFF80088694-20A3250E@9.40.1.30
sip_msgs: Enabled.. Total Traces logged = 7
sip_fsm: Enabled.. Total Traces logged = 26
sip_apis: Enabled.. Total Traces logged = 19
sip_misc: Enabled.. Total Traces logged = 3
-------------------------------
*Jul  2 13:16:30.122: API Name = voip_rtp_allocate_port Port = 16386
*Jul  2 13:16:30.122: API Name = voip_rtp_create_session Ret_code= 0
*Jul  2 13:16:30.122: API Name = voip_rtp_set_non_rtp_call Ret_code= 0
*Jul  2 13:16:30.123: API Name = voip_rtp_update_callinfo Ret_code= 0
*Jul  2 13:16:30.124: API Name = cc_api_update_interface_cac_resource Ret_code= 0
*Jul  2 13:16:30.124: API Name = cc_api_call_proceeding Ret_code= 0
*Jul  2 13:16:30.126: API Name = voip_rtp_update_callinfo Ret_code= 0
*Jul  2 13:16:30.126: API Name = voip_rtp_set_non_rtp_call Ret_code= 0
*Jul  2 13:16:30.126: API Name = voip_rtp_update_callinfo Ret_code= 0
*Jul  2 13:16:30.128: API Name = cc_api_call_alert Ret_code= 0
*Jul  2 13:16:30.128: API Name = cc_api_call_mode_update_ind Ret_code= 0
*Jul  2 13:16:30.129: API Name = cc_api_caps_ind Ret_code= 0
*Jul  2 13:16:30.129: API Name = cc_api_call_connected Ret_code= 0
*Jul  2 13:16:30.129: API Name = voip_rtp_update_callinfo Ret_code= 0
*Jul  2 13:16:30.131: API Name = voip_rtp_update_callinfo Ret_code= 0
*Jul  2 13:16:30.131: API Name = voip_rtp_set_non_rtp_call Ret_code= 0
*Jul  2 13:16:30.131: API Name = voip_rtp_update_callinfo Ret_code= 0
*Jul  2 13:16:30.131: API Name = cc_api_bridge_done Ret_code= 0
*Jul  2 13:16:30.131: API Name = ccsip_bridge Ret_code= 0
--------Cover buff----------
        buffer-id = 3   ccCallId = 3    PeerCallId = 4
        Called-Number = 44444   Calling-Number = 33333  Sip-Call-Id = 1-5682@9.40.1.22
sip_msgs: Enabled.. Total Traces logged = 8
sip_fsm: Enabled.. Total Traces logged = 22
sip_apis: Enabled.. Total Traces logged = 15
sip_misc: Enabled.. Total Traces logged = 4
-------------------------------
*Jul  2 13:21:40.322: API Name = cc_api_update_interface_cac_resource Ret_code= 0
*Jul  2 13:21:40.322: API Name = voip_rtp_allocate_port Port = 16388
*Jul  2 13:21:40.322: API Name = cc_api_call_setup_ind_with_callID Ret_code= 0
*Jul  2 13:21:40.324: API Name = voip_rtp_create_session Ret_code= 0
*Jul  2 13:21:40.324: API Name = voip_rtp_set_non_rtp_call Ret_code= 0
*Jul  2 13:21:40.324: API Name = voip_rtp_update_callinfo Ret_code= 0
*Jul  2 13:21:40.330: API Name = cc_api_caps_ack Ret_code= 0
*Jul  2 13:21:40.331: API Name = cc_api_caps_ack Ret_code= 0
*Jul  2 13:21:40.333: API Name = voip_rtp_update_callinfo Ret_code= 0
*Jul  2 13:21:40.333: API Name = cc_api_call_mode_update_ind Ret_code= 0
*Jul  2 13:21:40.333: API Name = voip_rtp_update_callinfo Ret_code= 0
*Jul  2 13:21:40.333: API Name = voip_rtp_set_non_rtp_call Ret_code= 0
*Jul  2 13:21:40.334: API Name = voip_rtp_update_callinfo Ret_code= 0
*Jul  2 13:21:40.334: API Name = cc_api_bridge_done Ret_code= 0
*Jul  2 13:21:40.332: API Name = ccsip_bridge Ret_code= 0
--------Cover buff----------
        buffer-id = 4   ccCallId = 4    PeerCallId = 3
        Called-Number = 44444   Calling-Number = 33333  Sip-Call-Id =
2A3AEE9D-FFFFFFFFE25111E2-FFFFFFFF800F8694-20A3250E@9.40.1.30
sip_msgs: Enabled.. Total Traces logged = 7
sip_fsm: Enabled.. Total Traces logged = 26
sip_apis: Enabled.. Total Traces logged = 19
sip_misc: Enabled.. Total Traces logged = 3
-------------------------------
*Jul  2 13:21:40.324: API Name = voip_rtp_allocate_port Port = 16390
*Jul  2 13:21:40.326: API Name = voip_rtp_create_session Ret_code= 0
*Jul  2 13:21:40.326: API Name = voip_rtp_set_non_rtp_call Ret_code= 0
*Jul  2 13:21:40.326: API Name = voip_rtp_update_callinfo Ret_code= 0
```

```
*Jul  2 13:21:40.327: API Name = cc_api_update_interface_cac_resource Ret_code= 0
*Jul  2 13:21:40.327: API Name = cc_api_call_proceeding Ret_code= 0
*Jul  2 13:21:40.328: API Name = voip_rtp_update_callinfo Ret_code= 0
*Jul  2 13:21:40.327: API Name = voip_rtp_set_non_rtp_call Ret_code= 0
*Jul  2 13:21:40.327: API Name = voip_rtp_update_callinfo Ret_code= 0
*Jul  2 13:21:40.329: API Name = cc_api_call_alert Ret_code= 0
*Jul  2 13:21:40.330: API Name = cc_api_call_mode_update_ind Ret_code= 0
*Jul  2 13:21:40.331: API Name = cc_api_caps_ind Ret_code= 0
*Jul  2 13:21:40.331: API Name = cc_api_call_connected Ret_code= 0
*Jul  2 13:21:40.331: API Name = voip_rtp_update_callinfo Ret_code= 0
*Jul  2 13:21:40.333: API Name = voip_rtp_update_callinfo Ret_code= 0
*Jul  2 13:21:40.333: API Name = voip_rtp_set_non_rtp_call Ret_code= 0
*Jul  2 13:21:40.333: API Name = voip_rtp_update_callinfo Ret_code= 0
*Jul  2 13:21:40.333: API Name = cc_api_bridge_done Ret_code= 0
*Jul  2 13:21:40.333: API Name = ccsip_bridge Ret_code= 0
```

In the following example, there are two active calls on Cisco UBE. In the first call, the calling number is 1111 and it calls the number 22222. In the second call, the calling number is 33333 and it calls number 44444. The example shows how to filter the API event traces where the calling number is 11111:

```
Device# show monitor event-trace voip ccsip api filter calling-num 11111 all
--------Cover buff----------
        buffer-id = 1   ccCallId = 1    PeerCallId = 2
        Called-Number = 22222   Calling-Number = 11111  Sip-Call-Id = 1-5671@9.40.1.22
sip_msgs: Enabled.. Total Traces logged = 8
sip_fsm: Enabled.. Total Traces logged = 22
sip_apis: Enabled.. Total Traces logged = 15
sip_misc: Enabled.. Total Traces logged = 4
--------------------------------
*Jul  2 13:16:30.119: API Name = cc_api_update_interface_cac_resource Ret_code= 0
*Jul  2 13:16:30.119: API Name = voip_rtp_allocate_port Port = 16384
*Jul  2 13:16:30.120: API Name = cc_api_call_setup_ind_with_callID Ret_code= 0
*Jul  2 13:16:30.123: API Name = voip_rtp_create_session Ret_code= 0
*Jul  2 13:16:30.123: API Name = voip_rtp_set_non_rtp_call Ret_code= 0
*Jul  2 13:16:30.123: API Name = voip_rtp_update_callinfo Ret_code= 0
*Jul  2 13:16:30.129: API Name = cc_api_caps_ack Ret_code= 0
*Jul  2 13:16:30.130: API Name = cc_api_caps_ack Ret_code= 0
*Jul  2 13:16:30.131: API Name = voip_rtp_update_callinfo Ret_code= 0
*Jul  2 13:16:30.131: API Name = cc_api_call_mode_update_ind Ret_code= 0
*Jul  2 13:16:30.131: API Name = voip_rtp_update_callinfo Ret_code= 0
*Jul  2 13:16:30.131: API Name = voip_rtp_set_non_rtp_call Ret_code= 0
*Jul  2 13:16:30.131: API Name = voip_rtp_update_callinfo Ret_code= 0
*Jul  2 13:16:30.131: API Name = cc_api_bridge_done Ret_code= 0
*Jul  2 13:16:30.131: API Name = ccsip_bridge Ret_code= 0
--------Cover buff----------
        buffer-id = 2   ccCallId = 2    PeerCallId = 1
        Called-Number = 22222   Calling-Number = 11111  Sip-Call-Id =
7155B639-FFFFFFFFE25011E2-FFFFFFFF80088694-20A3250E@9.40.1.30
sip_msgs: Enabled.. Total Traces logged = 7
sip_fsm: Enabled.. Total Traces logged = 26
sip_apis: Enabled.. Total Traces logged = 19
sip_misc: Enabled.. Total Traces logged = 3
--------------------------------
*Jul  2 13:16:30.123: API Name = voip_rtp_allocate_port Port = 16386
*Jul  2 13:16:30.124: API Name = voip_rtp_create_session Ret_code= 0
*Jul  2 13:16:30.124: API Name = voip_rtp_set_non_rtp_call Ret_code= 0
*Jul  2 13:16:30.124: API Name = voip_rtp_update_callinfo Ret_code= 0
*Jul  2 13:16:30.124: API Name = cc_api_update_interface_cac_resource Ret_code= 0
*Jul  2 13:16:30.124: API Name = cc_api_call_proceeding Ret_code= 0
*Jul  2 13:16:30.126: API Name = voip_rtp_update_callinfo Ret_code= 0
*Jul  2 13:16:30.126: API Name = voip_rtp_set_non_rtp_call Ret_code= 0
*Jul  2 13:16:30.126: API Name = voip_rtp_update_callinfo Ret_code= 0
```

```
*Jul  2 13:16:30.128: API Name = cc_api_call_alert Ret_code= 0
*Jul  2 13:16:30.129: API Name = cc_api_call_mode_update_ind Ret_code= 0
*Jul  2 13:16:30.130: API Name = cc_api_caps_ind Ret_code= 0
*Jul  2 13:16:30.129: API Name = cc_api_call_connected Ret_code= 0
*Jul  2 13:16:30.129: API Name = voip_rtp_update_callinfo Ret_code= 0
*Jul  2 13:16:30.131: API Name = voip_rtp_update_callinfo Ret_code= 0
*Jul  2 13:16:30.131: API Name = voip_rtp_set_non_rtp_call Ret_code= 0
*Jul  2 13:16:30.131: API Name = voip_rtp_update_callinfo Ret_code= 0
*Jul  2 13:16:30.131: API Name = cc_api_bridge_done Ret_code= 0
*Jul  2 13:16:30.131: API Name = ccsip_bridge Ret_code= 0
```

The following example shows how to display the traces captured for completed calls. The call could be a successful one or a failed one. The output displays all the traces (fsm, msg, misc, api) that were enabled at the time of call, arranged according to time stamp:

```
Device# show monitor event-trace voip ccsip history all
--------Cover buff----------
        buffer-id = 2   ccCallId = 2    PeerCallId = 1
        Called-Number = 22222   Calling-Number = 11111  Sip-Call-Id =
7155B639-FFFFFFFFE25011E2-FFFFFFFF80088694-20A3250E@9.40.1.30
sip_msgs: Enabled.. Total Traces logged = 9
sip_fsm: Enabled.. Total Traces logged = 31
sip_apis: Enabled.. Total Traces logged = 25
sip_misc: Enabled.. Total Traces logged = 3
------------------------------
*Jul  2 13:16:30.122: sip_misc: Outbound dial-peer matched : tag = 22222
*Jul  2 13:16:30.122: sip_fsm: FSM TYPE = SIP STATE TRANS FSM Current State = STATE_NONE
Next State = STATE_IDLE Current Substate = STATE_NONE Next Substate = STATE_IDLE
*Jul  2 13:16:30.122: sip_fsm: CNFSM TYPE = SIP IWF CNFSM, Event = E_SIP_IWF_EV_SET_MODE,
      Current State = CNFSM_CONTAINER_STATE,      Next State = CNFSM_NO_STATE_CHANGE
*Jul  2 13:16:30.122: sip_fsm: CNFSM TYPE = SIP IWF CNFSM, Event = E_SIP_IWF_EV_PRE_SETUP,
      Current State = S_SIP_IWF_SDP_IDLE,         Next State = CNFSM_NO_STATE_CHANGE
*Jul  2 13:16:30.123: sip_fsm: CNFSM TYPE = SIP IWF CNFSM, Event =
E_SIP_IWF_EV_PEER_MULTIMEDIA_CHANNEL_IND,    Current State = S_SIP_IWF_SDP_IDLE,
Next State = CNFSM_NO_STATE_CHANGE
*Jul  2 13:16:30.123: sip_misc: Media Stream Index = 1, Media Stream Type = voice-only
Stream State = STREAM_ADDING
        Negotiated Codec = No Codec    Negotiated DTMF Type = inband-voice
*Jul  2 13:16:30.122: sip_fsm: CNFSM TYPE = SIP Media Service CNFSM, Event =
E_IPIP_MEDIA_SERV_EV_PEER_CHNL_IND,        Current State = S_IPIP_MEDIA_SERV_STATE_IDLE,
     Next State = S_IPIP_MEDIA_SERV_STATE_INIT_XCODER_RESERVED
*Jul  2 13:16:30.122: sip_fsm: CNFSM TYPE = SIP IWF CNFSM, Event =
E_SIP_IWF_EV_CONTINUE_PRE_SETUP,     Current State = S_SIP_IWF_SDP_IDLE,         Next State
 = CNFSM_NO_STATE_CHANGE
*Jul  2 13:16:30.123: sip_fsm: CNFSM TYPE = SIP Media Service CNFSM, Event =
E_IPIP_MEDIA_SERV_EV_XCODER_RESET_STREAM,  Current State = CNFSM_CONTAINER_STATE,      Next
 State = S_IPIP_MEDIA_SERV_STATE_IDLE
*Jul  2 13:16:30.124: sip_fsm: CNFSM TYPE = SIP IWF CNFSM, Event =
E_SIP_IWF_EV_INIT_CALL_SETUP,        Current State = S_SIP_IWF_SDP_IDLE,         Next State
 = CNFSM_NO_STATE_CHANGE
*Jul  2 13:16:30.124: sip_apis: API Name = voip_rtp_allocate_port Port = 16386
*Jul  2 13:16:30.124: sip_apis: API Name = voip_rtp_create_session Ret_code= 0
*Jul  2 13:16:30.124: sip_apis: API Name = voip_rtp_set_non_rtp_call Ret_code= 0
*Jul  2 13:16:30.124: sip_apis: API Name = voip_rtp_update_callinfo Ret_code= 0
*Jul  2 13:16:30.124: sip_apis: API Name = cc_api_update_interface_cac_resource Ret_code=
0
*Jul  2 13:16:30.124: sip_fsm:  FSM TYPE = SIP Event-state FSM, Event =
SIPSPI_EV_CC_CALL_SETUP          Current State = STATE_IDLE
*Jul  2 13:16:30.124: sip_apis: API Name = cc_api_call_proceeding Ret_code= 0
*Jul  2 13:16:30.125: sip_fsm: CNFSM TYPE = SIP Offer-Answer CNFSM, Event =
E_SIP_INVITE_SDP_SENT,      Current State = S_SIP_EARLY_DIALOG_IDLE,    Next State =
S_SIP_EARLY_DIALOG_OFFER_SENT
*Jul  2 13:16:30.125: sip_fsm: CNFSM TYPE = SIP IWF CNFSM, Event = E_SIP_IWF_EV_SENT_SDP,
```

```
      Current State = S_SIP_IWF_SDP_IDLE,         Next State = S_SIP_IWF_SDP_SENT_AWAIT_SDP
*Jul  2 13:16:30.126: sip_fsm: FSM TYPE = SIP STATE TRANS FSM Current State = STATE_IDLE
Next State = STATE_SENT_INVITE Current Substate = STATE_IDLE Next Substate = STATE_SENT_INVITE
*Jul  2 13:16:30.125: sip_apis: API Name = voip_rtp_update_callinfo Ret_code= 0
*Jul  2 13:16:30.125: sip_apis: API Name = voip_rtp_set_non_rtp_call Ret_code= 0
*Jul  2 13:16:30.125: sip_apis: API Name = voip_rtp_update_callinfo Ret_code= 0
*Jul  2 13:16:30.125: sip_msgs: SIP_MSG: Fragment Number = 1,  Message Id = 3, Last Fragment
 = No, Messages Direction = Sent, Message:
INVITE sip:22222@9.40.1.22:9632 SIP/2.0
Via: SIP/2.0/UDP 9.40.1.30:5060;branch=z9hG4bK07AC
Remote-Party-ID: "11111 " <sip:11111@9.40.1.30>;party=calling;screen=no;privacy=off
From: "11111 " <sip:11111@9.40.1.30>;tag=38C94-2507
To: <sip:22222@9.40.1.22>
Date: Tue, 02 Jul 2013 13:16:30 GMT
Call-ID: 7155B639-FFFFFFFFE25011E2-FFFFFFFF80088694-20A3250E@9.40.1.30
Supported: 100rel,timer,resource-priority,replaces,sdp-anat
Min-SE:  1800
Cisco-Guid: 1901362665-3796898274-2147649172-0547562766
--------

*Jul  2 13:16:30.126: sip_msgs: SIP_MSG: Fragment Number = 2,  Message Id = 3, Last Fragment
 = No, Messages Direction = Sent, Message:

User-Agent: Cisco-SIPGateway/IOS-15.3.20130514.122658.
Allow: INVITE, OPTIONS, BYE, CANCEL, ACK, PRACK, UPDATE, REFER, SUBSCRIBE, NOTIFY, INFO,
REGISTER
CSeq: 101 INVITE
Timestamp: 1372770990
Contact: <sip:11111@9.40.1.30:5060>
Expires: 180
Allow-Events: telephone-event
Max-Forwards: 69
Content-Type: application/sdp
Content-Disposition: session;handling=required
Content-Length: 206

v=0
o=CiscoSystemsSIP-GW-UserAgent 5243 1933 IN IP4 9.40.1.30
s=SIP Call
c=IN IP4 9.40.1.30
t=0
--------

*Jul  2 13:16:30.126: sip_msgs: SIP_MSG: Fragment Number = 3,  Message Id = 3, Last Fragment
 = Yes, Messages Direction = Sent, Message:
0
m=audio 16386 RTP/AVP 0 19
c=IN IP4 9.40.1.30
a=rtpmap:0 PCMU/8000
a=rtpmap:19 CN/8000
a=ptime:20

--------

*Jul  2 13:16:30.126: sip_msgs: SIP_MSG: Fragment Number = 1,  Message Id = 4, Last Fragment
 = Yes, Messages Direction = received, Message:
SIP/2.0 180 Ringing
Via: SIP/2.0/UDP 9.40.1.30:5060;branch=z9hG4bK07AC
From: "11111 " <sip:11111@9.40.1.30>;tag=38C94-2507
To: <sip:22222@9.40.1.22>;tag=4
Call-ID: 7155B639-FFFFFFFFE25011E2-FFFFFFFF80088694-20A3250E@9.40.1.30
CSeq: 101 INVITE
Contact: <sip:9.40.1.22:9632;transport=UDP>
Content-Length: 0
```

```
--------

*Jul  2 13:16:30.127: sip_fsm:  FSM TYPE = SIP Event-state FSM, Event = SIPSPI_EV_NEW_MESSAGE
          Current State = STATE_SENT_INVITE
*Jul  2 13:16:30.127: sip_apis: API Name = cc_api_call_alert Ret_code= 0
*Jul  2 13:16:30.128: sip_fsm: FSM TYPE = SIP STATE TRANS FSM Current State =
STATE_SENT_INVITE Next State = STATE_RECD_PROCEEDING Current Substate = STATE_SENT_INVITE
Next Substate = STATE_RECD_PROCEEDING
*Jul  2 13:16:30.128: sip_msgs: SIP_MSG: Fragment Number = 1,  Message Id = 6, Last Fragment
 = No, Messages Direction = received, Message:
SIP/2.0 200 OK
Via: SIP/2.0/UDP 9.40.1.30:5060;branch=z9hG4bK07AC
From: "11111 " <sip:11111@9.40.1.30>;tag=38C94-2507
To: <sip:22222@9.40.1.22>;tag=4
Call-ID: 7155B639-FFFFFFFFE25011E2-FFFFFFFF80088694-20A3250E@9.40.1.30
CSeq: 101 INVITE
Contact: <sip:9.40.1.22:9632;transport=UDP>
Content-Type: application/sdp
Content-Length:   199

v=0

o=user1 53655765 2353687637 IN IP4 9.40.1.22
s=-
c=IN IP4 9.40.1.22
t=0 0
m=audio 9832 RTP/AVP 0 101
a=rtpmap:0 PCMU/8000
a=rtpmap:101 telephon
--------

*Jul  2 13:16:30.128: sip_msgs: SIP_MSG: Fragment Number = 2,  Message Id = 6, Last Fragment
 = Yes, Messages Direction = received, Message:
e-event/8000
a=fmtp:101 0-16
a=ptime:20


--------

*Jul  2 13:16:30.129: sip_fsm:  FSM TYPE = SIP Event-state FSM, Event = SIPSPI_EV_NEW_MESSAGE
          Current State = STATE_RECD_PROCEEDING
*Jul  2 13:16:30.129: sip_fsm: CNFSM TYPE = SIP Offer-Answer CNFSM, Event =
E_SIP_INVITE_RESP_SDP_RCVD, Current State = S_SIP_EARLY_DIALOG_OFFER_SENT,      Next State
 = S_SIP_EARLY_DIALOG_OFFER_ANSWER_COMPLETE
*Jul  2 13:16:30.129: sip_fsm: CNFSM TYPE = SIP IWF CNFSM, Event = E_SIP_IWF_EV_RCVD_SDP,
      Current State = S_SIP_IWF_SDP_SENT_AWAIT_SDP,       Next State = S_SIP_IWF_SDP_DONE
*Jul  2 13:16:30.128: sip_misc: Media Stream Index = 1, Media Stream Type = voice-only
Stream State = STREAM_ADDING
       Negotiated Codec = g711ulaw Negotiated DTMF Type = inband-voice
*Jul  2 13:16:30.128: sip_apis: API Name = cc_api_call_mode_update_ind Ret_code= 0
*Jul  2 13:16:30.129: sip_apis: API Name = cc_api_caps_ind Ret_code= 0
*Jul  2 13:16:30.129: sip_fsm: FSM TYPE = SIP STATE TRANS FSM Current State =
STATE_RECD_PROCEEDING Next State = STATE_RECD_PROCEEDING Current Substate =
STATE_RECD_PROCEEDING Next Substate = STATE_RECD_PROCEEDING
*Jul  2 13:16:30.130: sip_apis: API Name = cc_api_call_connected Ret_code= 0
*Jul  2 13:16:30.130: sip_fsm: FSM TYPE = SIP STATE TRANS FSM Current State =
STATE_RECD_PROCEEDING Next State = SIP_STATE_RECD_SUCCESS Current Substate =
STATE_RECD_PROCEEDING Next Substate = SIP_STATE_RECD_SUCCESS
*Jul  2 13:16:30.130: sip_fsm: CNFSM TYPE = SIP Offer-Answer CNFSM, Event = E_SIP_DIALOG_ESTD,
  Current State = S_SIP_EARLY_DIALOG_OFFER_ANSWER_COMPLETE,   Next State =
```

```
S_SIP_MID_DIALOG_IDLE
*Jul  2 13:16:30.130: sip_fsm: CNFSM TYPE = SIP IWF CNFSM, Event = E_SIP_IWF_EV_CALL_ACTIVE,
    Current State = CNFSM_CONTAINER_STATE,      Next State = CNFSM_NO_STATE_CHANGE
*Jul  2 13:16:30.130: sip_fsm: FSM TYPE = SIP STATE TRANS FSM Current State =
SIP_STATE_RECD_SUCCESS Next State = STATE_ACTIVE Current Substate = SIP_STATE_RECD_SUCCESS
 Next Substate = STATE_ACTIVE
*Jul  2 13:16:30.129: sip_fsm: CNFSM TYPE = SIP IWF CNFSM, Event =
E_SIP_IWF_EV_UPDATE_STREAM_CONTEXT,  Current State = S_SIP_IWF_SDP_DONE,        Next State
 = CNFSM_NO_STATE_CHANGE
*Jul  2 13:16:30.129: sip_apis: API Name = voip_rtp_update_callinfo Ret_code= 0
*Jul  2 13:16:30.130: sip_fsm: CNFSM TYPE = SIP IWF CNFSM, Event =
E_SIP_IWF_EV_PEER_CAPS_ACK,, Current State = CNFSM_CONTAINER_STATE,      Next State =
CNFSM_NO_STATE_CHANGE
*Jul  2 13:16:30.130: sip_fsm: CNFSM TYPE = SIP IWF CNFSM, Event =
E_SIP_IWF_EV_PEER_CAPS_ACK,, Current State = CNFSM_CONTAINER_STATE,      Next State =
CNFSM_NO_STATE_CHANGE
*Jul  2 13:16:30.131: sip_fsm: CNFSM TYPE = SIP Media Service CNFSM, Event =
E_IPIP_MEDIA_SERV_EV_CALL_ACTIVE,  Current State = CNFSM_CONTAINER_STATE,      Next State
= CNFSM_NO_STATE_CHANGE
*Jul  2 13:16:30.131: sip_msgs: SIP_MSG: Fragment Number = 1,  Message Id = 7, Last Fragment
 = Yes, Messages Direction = Sent, Message:
ACK sip:9.40.1.22:9632;transport=UDP SIP/2.0
Via: SIP/2.0/UDP 9.40.1.30:5060;branch=z9hG4bK113B1
From: "11111 " <sip:11111@9.40.1.30>;tag=38C94-2507
To: <sip:22222@9.40.1.22>;tag=4
Date: Tue, 02 Jul 2013 13:16:30 GMT
Call-ID: 7155B639-FFFFFFFFE25011E2-FFFFFFFF80088694-20A3250E@9.40.1.30
Max-Forwards: 70
CSeq: 101 ACK

Allow-Events: telephone-event
Content-Length: 0


--------

*Jul  2 13:16:30.132: sip_apis: API Name = voip_rtp_update_callinfo Ret_code= 0
*Jul  2 13:16:30.132: sip_apis: API Name = voip_rtp_set_non_rtp_call Ret_code= 0
*Jul  2 13:16:30.132: sip_apis: API Name = voip_rtp_update_callinfo Ret_code= 0
*Jul  2 13:16:30.132: sip_apis: API Name = cc_api_bridge_done Ret_code= 0
*Jul  2 13:16:30.132: sip_apis: API Name = ccsip_bridge Ret_code= 0
*Jul  2 13:32:52.831: sip_fsm: CNFSM TYPE = SIP Media Service CNFSM, Event =
E_IPIP_MEDIA_SERV_EV_XCODER_RESET_STREAM,  Current State = CNFSM_CONTAINER_STATE,      Next
 State = S_IPIP_MEDIA_SERV_STATE_IDLE
*Jul  2 13:32:52.831: sip_apis: API Name = voip_rtp_update_callinfo Ret_code= 0
*Jul  2 13:32:52.832: sip_apis: API Name = cc_api_bridge_drop_done Ret_code= 0
*Jul  2 13:32:52.833: sip_apis: API Name = cc_api_update_interface_cac_resource Ret_code=
0
*Jul  2 13:32:52.833: sip_fsm:  FSM TYPE = SIP Event-state FSM, Event =
SIPSPI_EV_CC_CALL_DISCONNECT    Current State = STATE_ACTIVE
*Jul  2 13:32:52.833: sip_fsm: FSM TYPE = SIP STATE TRANS FSM Current State = STATE_ACTIVE
 Next State = STATE_DISCONNECTING Current Substate = STATE_ACTIVE Next Substate =
STATE_DISCONNECTING
*Jul  2 13:32:52.831: sip_msgs: SIP_MSG: Fragment Number = 1,  Message Id = 21, Last Fragment
 = Yes, Messages Direction = Sent, Message:
BYE sip:9.40.1.22:9632;transport=UDP SIP/2.0
Via: SIP/2.0/UDP 9.40.1.30:5060;branch=z9hG4bK4326
From: "11111 " <sip:11111@9.40.1.30>;tag=38C94-2507
To: <sip:22222@9.40.1.22>;tag=4
Date: Tue, 02 Jul 2013 13:16:30 GMT
Call-ID: 7155B639-FFFFFFFFE25011E2-FFFFFFFF80088694-20A3250E@9.40.1.30
User-Agent: Cisco-SIPGateway/IOS-15.3.20130514.122658.
Max-Forwards: 70
Timestamp: 1372771972
```

```
CSeq: 102 BYE
Reason: Q.850;cause=16
Content-Length: 0


--------

*Jul  2 13:32:52.839: sip_msgs: SIP_MSG: Fragment Number = 1,  Message Id = 22, Last Fragment
 = Yes, Messages Direction = received, Message:
SIP/2.0 200 OK
Via: SIP/2.0/UDP 9.40.1.30:5060;branch=z9hG4bK4326
From: "11111 " <sip:11111@9.40.1.30>;tag=38C94-2507

To: <sip:22222@9.40.1.22>;tag=4;tag=4
Call-ID: 7155B639-FFFFFFFFE25011E2-FFFFFFFF80088694-20A3250E@9.40.1.30
CSeq: 102 BYE
Contact: <sip:9.40.1.22:9632;transport=UDP>


--------

*Jul  2 13:32:52.838: sip_fsm:  FSM TYPE = SIP Event-state FSM, Event = SIPSPI_EV_NEW_MESSAGE
           Current State = STATE_DISCONNECTING
*Jul  2 13:32:52.838: sip_apis: API Name = voip_rtp_delete_dp_session Ret_code= 0
*Jul  2 13:32:52.851: sip_apis: API Name = ccsip_voip_rtp_fpi_event_handler Ret_code= 0
*Jul  2 13:32:52.851: sip_apis: API Name = cc_api_call_disconnect_done Ret_code= 0
*Jul  2 13:32:52.851: sip_fsm: FSM TYPE = SIP STATE TRANS FSM Current State =
STATE_DISCONNECTING Next State = STATE_DEAD Current Substate = STATE_DISCONNECTING Next
Substate = STATE_DEAD
--------Cover buff----------
        buffer-id = 1   ccCallId = 1    PeerCallId = 2
        Called-Number = 22222   Calling-Number = 11111  Sip-Call-Id = 1-5671@9.40.1.22
sip_msgs: Enabled.. Total Traces logged = 10
sip_fsm: Enabled.. Total Traces logged = 28
sip_apis: Enabled.. Total Traces logged = 23
sip_misc: Enabled.. Total Traces logged = 4
-------------------------------
*Jul  2 13:16:30.117: sip_msgs: SIP_MSG: Fragment Number = 1,  Message Id = 1, Last Fragment
 = No, Messages Direction = received, Message:
INVITE sip:22222@9.40.1.30:5060 SIP/2.0
Via: SIP/2.0/UDP 9.40.1.22:9232;branch=z9hG4bK-5671-1-0
From: 11111 <sip:11111@9.40.1.22:9232>;tag=1
To: 22222 <sip:22222@9.40.1.30:5060>
Call-ID: 1-5671@9.40.1.22
CSeq: 1 INVITE
Contact: <sip:11111@9.40.1.22:9232>
Max-Forwards: 70
Subject: Call Spike Testing
Content-Length:  182
Content-Type: application/sdp

v=0
o=- 53655765 2353687637 IN IP4 9.40.1.22
s=-
c=IN IP4 9.40.1.22

t=0 0
m=audio 9432 RTP/AVP 0 101
a=rtpmap:0 PCMU/8000
a=rtpm
--------

*Jul  2 13:16:30.115: sip_msgs: SIP_MSG: Fragment Number = 2,  Message Id = 1, Last Fragment
 = Yes, Messages Direction = received, Message:
```

```
ap: 101 telephone-event/8000
a=fmtp:101 0-16

--------

*Jul  2 13:16:30.115: sip_fsm: FSM TYPE = SIP STATE TRANS FSM Current State = STATE_NONE
Next State = STATE_IDLE Current Substate = STATE_NONE Next Substate = STATE_IDLE
*Jul  2 13:16:30.118: sip_misc: Inbound dial-peer matched : tag = 11111
*Jul  2 13:16:30.119: sip_fsm: CNFSM TYPE = SIP Offer-Answer CNFSM, Event =
E_SIP_INVITE_SDP_RCVD,      Current State = S_SIP_EARLY_DIALOG_IDLE,    Next State =
S_SIP_EARLY_DIALOG_OFFER_RCVD
*Jul  2 13:16:30.119: sip_fsm: CNFSM TYPE = SIP IWF CNFSM, Event = E_SIP_IWF_EV_RCVD_SDP,
      Current State = S_SIP_IWF_SDP_IDLE,         Next State =
S_SIP_IWF_SDP_RCVD_AWAIT_PEER_EVENT
*Jul  2 13:16:30.119: sip_misc: Media Stream Index = 1, Media Stream Type = voice-only
Stream State = STREAM_ADDING
        Negotiated Codec = g711ulaw Negotiated DTMF Type = inband-voice
*Jul  2 13:16:30.119: sip_apis: API Name = cc_api_update_interface_cac_resource Ret_code=
0
*Jul  2 13:16:30.119: sip_apis: API Name = voip_rtp_allocate_port Port = 16384
*Jul  2 13:16:30.120: sip_misc: Media Stream Index = 1, Media Stream Type = voice-only
Stream State = STREAM_ADDING
        Negotiated Codec = g711ulaw Negotiated DTMF Type = inband-voice
*Jul  2 13:16:30.119: sip_apis: API Name = cc_api_call_setup_ind_with_callID Ret_code= 0
*Jul  2 13:16:30.119: sip_fsm: FSM TYPE = SIP STATE TRANS FSM Current State = STATE_IDLE
Next State = STATE_RECD_INVITE Current Substate = STATE_IDLE Next Substate = STATE_RECD_INVITE
*Jul  2 13:16:30.121: sip_fsm: CNFSM TYPE = SIP IWF CNFSM, Event = E_SIP_IWF_EV_SET_MODE,
      Current State = CNFSM_CONTAINER_STATE,      Next State = CNFSM_NO_STATE_CHANGE
*Jul  2 13:16:30.123: sip_apis: API Name = voip_rtp_create_session Ret_code= 0
*Jul  2 13:16:30.123: sip_apis: API Name = voip_rtp_set_non_rtp_call Ret_code= 0
*Jul  2 13:16:30.123: sip_apis: API Name = voip_rtp_update_callinfo Ret_code= 0
*Jul  2 13:16:30.123: sip_fsm:  FSM TYPE = SIP Event-state FSM, Event =
SIPSPI_EV_CC_CALL_PROCEEDING    Current State = STATE_RECD_INVITE
*Jul  2 13:16:30.123: sip_fsm: CNFSM TYPE = SIP Media Service CNFSM, Event =
E_IPIP_MEDIA_SERV_EV_XCODER_RESET_STREAM,  Current State = CNFSM_CONTAINER_STATE,      Next
 State = S_IPIP_MEDIA_SERV_STATE_IDLE
*Jul  2 13:16:30.126: sip_msgs: SIP_MSG: Fragment Number = 1,  Message Id = 2, Last Fragment
 = Yes, Messages Direction = Sent, Message:
SIP/2.0 100 Trying
Via: SIP/2.0/UDP 9.40.1.22:9232;branch=z9hG4bK-5671-1-0
From: 11111 <sip:11111@9.40.1.22:9232>;tag=1
To: 22222 <sip:22222@9.40.1.30:5060>
Date: Tue, 02 Jul 2013 13:16:30 GMT
Call-ID: 1-5671@9.40.1.22
CSeq: 1 INVITE
Allow-Events: telephone-event
Server: Cisco-SIPGateway/IOS-15.3.20130514.122658.
Content-Length: 0


--------

*Jul  2 13:16:30.127: sip_fsm:  FSM TYPE = SIP Event-state FSM, Event =
SIPSPI_EV_CC_CALL_ALERTING      Current State = STATE_RECD_INVITE
*Jul  2 13:16:30.127: sip_fsm: FSM TYPE = SIP STATE TRANS FSM Current State =
STATE_RECD_INVITE Next State = STATE_SENT_ALERTING Current Substate = STATE_RECD_INVITE
Next Substate = STATE_SENT_ALERTING
*Jul  2 13:16:30.128: sip_msgs: SIP_MSG: Fragment Number = 1,  Message Id = 5, Last Fragment
 = No, Messages Direction = Sent, Message:
SIP/2.0 180 Ringing
Via: SIP/2.0/UDP 9.40.1.22:9232;branch=z9hG4bK-5671-1-0
From: 11111 <sip:11111@9.40.1.22:9232>;tag=1
To: 22222 <sip:22222@9.40.1.30:5060>;tag=38C97-1057
Date: Tue, 02 Jul 2013 13:16:30 GMT
```

```
Call-ID: 1-5671@9.40.1.22
CSeq: 1 INVITE
Allow: INVITE, OPTIONS, BYE, CANCEL, ACK, PRACK, UPDATE, REFER, SUBSCRIBE, NOTIFY, INFO,
REGISTER
Allow-Events: telephone-event
Remote-Party-ID: <sip:22222@9.40.1.30>;party=called;screen=no;privacy=off
Contact: <sip:22222@9.40.1.30:5060>

--------

*Jul  2 13:16:30.128: sip_msgs: SIP_MSG: Fragment Number = 2,  Message Id = 5, Last Fragment
 = Yes, Messages Direction = Sent, Message:
Server: Cisco-SIPGateway/IOS-15.3.20130514.122658.
Content-Length: 0


--------

*Jul  2 13:16:30.129: sip_fsm: CNFSM TYPE = SIP IWF CNFSM, Event = E_SIP_IWF_EV_PEER_CAPS,
      Current State = CNFSM_CONTAINER_STATE,      Next State = CNFSM_NO_STATE_CHANGE
*Jul  2 13:16:30.129: sip_apis: API Name = cc_api_caps_ack Ret_code= 0
*Jul  2 13:16:30.130: sip_apis: API Name = cc_api_caps_ack Ret_code= 0
*Jul  2 13:16:30.131: sip_fsm: CNFSM TYPE = SIP IWF CNFSM, Event =
E_SIP_IWF_EV_PEER_MULTIMEDIA_CHANNEL_ACK,    Current State =
S_SIP_IWF_SDP_RCVD_AWAIT_PEER_EVENT,        Next State = CNFSM_NO_STATE_CHANGE
*Jul  2 13:16:30.131: sip_misc: Media Stream Index = 1, Media Stream Type = voice-only
Stream State = STREAM_ADDING
        Negotiated Codec = g711ulaw Negotiated DTMF Type = inband-voice
*Jul  2 13:16:30.131: sip_apis: API Name = voip_rtp_update_callinfo Ret_code= 0
*Jul  2 13:16:30.131: sip_apis: API Name = cc_api_call_mode_update_ind Ret_code= 0
*Jul  2 13:16:30.131: sip_fsm: CNFSM TYPE = SIP Media Service CNFSM, Event =
E_IPIP_MEDIA_SERV_EV_PEER_CHNL_ACK,        Current State = S_IPIP_MEDIA_SERV_STATE_IDLE,
     Next State = CNFSM_NO_STATE_CHANGE
*Jul  2 13:16:30.132: sip_apis: API Name = voip_rtp_update_callinfo Ret_code= 0
*Jul  2 13:16:30.131: sip_apis: API Name = voip_rtp_set_non_rtp_call Ret_code= 0
*Jul  2 13:16:30.131: sip_apis: API Name = voip_rtp_update_callinfo Ret_code= 0
*Jul  2 13:16:30.131: sip_apis: API Name = cc_api_bridge_done Ret_code= 0
*Jul  2 13:16:30.131: sip_apis: API Name = ccsip_bridge Ret_code= 0
*Jul  2 13:16:30.139: sip_fsm: CNFSM TYPE = SIP IWF CNFSM, Event = E_SIP_IWF_EV_CALL_CONNECT,
   Current State = CNFSM_CONTAINER_STATE,      Next State = CNFSM_NO_STATE_CHANGE
*Jul  2 13:16:30.140: sip_fsm:  FSM TYPE = SIP Event-state FSM, Event =
SIPSPI_EV_CC_CALL_CONNECT       Current State = STATE_SENT_ALERTING
*Jul  2 13:16:30.140: sip_fsm: CNFSM TYPE = SIP Offer-Answer CNFSM, Event =
E_SIP_INVITE_RESP_SDP_SENT, Current State = S_SIP_EARLY_DIALOG_OFFER_RCVD,      Next State
 = S_SIP_EARLY_DIALOG_OFFER_ANSWER_COMPLETE
*Jul  2 13:16:30.140: sip_fsm: CNFSM TYPE = SIP IWF CNFSM, Event = E_SIP_IWF_EV_SENT_SDP,
      Current State = S_SIP_IWF_SDP_RCVD_AWAIT_PEER_EVENT,        Next State =
S_SIP_IWF_SDP_DONE
*Jul  2 13:16:30.141: sip_fsm: FSM TYPE = SIP STATE TRANS FSM Current State =
STATE_SENT_ALERTING Next State = STATE_SENT_SUCCESS Current Substate = STATE_SENT_ALERTING
 Next Substate = STATE_SENT_SUCCESS
*Jul  2 13:16:30.141: sip_msgs: SIP_MSG: Fragment Number = 1,  Message Id = 8, Last Fragment
 = No, Messages Direction = Sent, Message:
SIP/2.0 200 OK
Via: SIP/2.0/UDP 9.40.1.22:9232;branch=z9hG4bK-5671-1-0
From: 11111 <sip:11111@9.40.1.22:9232>;tag=1
To: 22222 <sip:22222@9.40.1.30:5060>;tag=38C97-1057
Date: Tue, 02 Jul 2013 13:16:30 GMT
Call-ID: 1-5671@9.40.1.22
CSeq: 1 INVITE
Allow: INVITE, OPTIONS, BYE, CANCEL, ACK, PRACK, UPDATE, REFER, SUBSCRIBE, NOTIFY, INFO,
REGISTER
Allow-Events: telephone-event
```

```
Remote-Party-ID: <sip:22222@9.40.1.30>;party=called;screen=no;privacy=off
Contact: <sip:22222@9.40.1.30:5060>
Suppo
--------

*Jul  2 13:16:30.142: sip_msgs: SIP_MSG: Fragment Number = 2,  Message Id = 8, Last Fragment
 = Yes, Messages Direction = Sent, Message:
rted: replaces
Supported: sdp-anat
Server: Cisco-SIPGateway/IOS-15.3.20130514.122658.
Supported: timer
Content-Type: application/sdp
Content-Disposition: session;handling=required
Content-Length: 182

v=0
o=CiscoSystemsSIP-GW-UserAgent 8289 9144 IN IP4 9.40.1.30
s=SIP Call
c=IN IP4 9.40.1.30
t=0 0
m=audio 16384 RTP/AVP 0
c=IN IP4 9.40.1.30

a=rtpmap:0 PCMU/8000
a=ptime:20

--------

*Jul  2 13:16:30.146: sip_msgs: SIP_MSG: Fragment Number = 1,  Message Id = 9, Last Fragment
 = Yes, Messages Direction = received, Message:
ACK sip:22222@9.40.1.30:5060 SIP/2.0
Via: SIP/2.0/UDP 9.40.1.22:9232;branch=z9hG4bK-5671-1-4
From: 11111 <sip:11111@9.40.1.22:9232>;tag=1
To: 22222 <sip:22222@9.40.1.30:5060>;tag=38C97-1057
Call-ID: 1-5671@9.40.1.22
CSeq: 1 ACK
Contact: sip:11111@9.40.1.22:9232
Max-Forwards: 70
Subject: Performance Test
Content-Type: application/sdp


--------

*Jul  2 13:16:30.146: sip_fsm:  FSM TYPE = SIP Event-state FSM, Event = SIPSPI_EV_NEW_MESSAGE
           Current State = STATE_SENT_SUCCESS
*Jul  2 13:16:30.146: sip_fsm: FSM TYPE = SIP STATE TRANS FSM Current State =
STATE_SENT_SUCCESS Next State = STATE_ACTIVE Current Substate = STATE_SENT_SUCCESS Next
Substate = STATE_ACTIVE
*Jul  2 13:16:30.146: sip_fsm: CNFSM TYPE = SIP Offer-Answer CNFSM, Event = E_SIP_DIALOG_ESTD,
  Current State = S_SIP_EARLY_DIALOG_OFFER_ANSWER_COMPLETE,   Next State =
S_SIP_MID_DIALOG_IDLE
*Jul  2 13:16:30.147: sip_fsm: CNFSM TYPE = SIP IWF CNFSM, Event = E_SIP_IWF_EV_CALL_ACTIVE,
    Current State = CNFSM_CONTAINER_STATE,      Next State = CNFSM_NO_STATE_CHANGE
*Jul  2 13:16:30.148: sip_fsm: CNFSM TYPE = SIP Media Service CNFSM, Event =
E_IPIP_MEDIA_SERV_EV_CALL_ACTIVE,  Current State = CNFSM_CONTAINER_STATE,      Next State
= CNFSM_NO_STATE_CHANGE
*Jul  2 13:32:52.829: sip_msgs: SIP_MSG: Fragment Number = 1,  Message Id = 19, Last Fragment
 = Yes, Messages Direction = received, Message:
BYE sip:22222@9.40.1.30:5060 SIP/2.0
Via: SIP/2.0/UDP 9.40.1.22:9232;branch=z9hG4bK-5671-1--1
From: 11111 <sip:11111@9.40.1.22:9232>;tag=1
To: 22222 <sip:22222@9.40.1.30:5060>;tag=38C97-1057
Call-ID: 1-5671@9.40.1.22
```

```
CSeq: 2 BYE
Max-Forwards: 70
Contact: <sip:9.40.1.22:9232;transport=UDP>
Content-Length: 0
--------

*Jul  2 13:32:52.829: sip_fsm:  FSM TYPE = SIP Event-state FSM, Event = SIPSPI_EV_NEW_MESSAGE
          Current State = STATE_ACTIVE
*Jul  2 13:32:52.830: sip_apis: API Name = cc_api_call_disconnected Ret_code= 0
*Jul  2 13:32:52.830: sip_fsm: FSM TYPE = SIP STATE TRANS FSM Current State = STATE_ACTIVE
 Next State = STATE_DISCONNECTING Current Substate = STATE_ACTIVE Next Substate =
STATE_DISCONNECTING
*Jul  2 13:32:52.830: sip_apis: API Name = voip_rtp_destroy_dp_session Ret_code= 0
*Jul  2 13:32:52.830: sip_fsm: CNFSM TYPE = SIP Media Service CNFSM, Event =
E_IPIP_MEDIA_SERV_EV_XCODER_RESET_STREAM,  Current State = CNFSM_CONTAINER_STATE,     Next
 State = S_IPIP_MEDIA_SERV_STATE_IDLE
*Jul  2 13:32:52.831: sip_apis: API Name = voip_rtp_update_callinfo Ret_code= 0
*Jul  2 13:32:52.831: sip_apis: API Name = cc_api_bridge_drop_done Ret_code= 0
*Jul  2 13:32:52.831: sip_apis: API Name = cc_api_update_interface_cac_resource Ret_code=
0
*Jul  2 13:32:52.831: sip_fsm:  FSM TYPE = SIP Event-state FSM, Event =
SIPSPI_EV_CC_CALL_DISCONNECT    Current State = STATE_DISCONNECTING
*Jul  2 13:32:52.832: sip_apis: API Name = voip_rtp_delete_dp_session Ret_code= 0
*Jul  2 13:32:52.831: sip_msgs: SIP_MSG: Fragment Number = 1,  Message Id = 20, Last Fragment
 = Yes, Messages Direction = Sent, Message:
SIP/2.0 200 OK
Via: SIP/2.0/UDP 9.40.1.22:9232;branch=z9hG4bK-5671-1--1
From: 11111 <sip:11111@9.40.1.22:9232>;tag=1
To: 22222 <sip:22222@9.40.1.30:5060>;tag=38C97-1057
Date: Tue, 02 Jul 2013 13:32:52 GMT
Call-ID: 1-5671@9.40.1.22
Server: Cisco-SIPGateway/IOS-15.3.20130514.122658.
CSeq: 2 BYE
Reason: Q.850;cause=16
Content-Length: 0

--------

*Jul  2 13:32:52.851: sip_apis: API Name = ccsip_voip_rtp_fpi_event_handler Ret_code= 0
*Jul  2 13:32:52.851: sip_apis: API Name = cc_api_call_disconnect_done Ret_code= 0
*Jul  2 13:32:52.851: sip_fsm: FSM TYPE = SIP STATE TRANS FSM Current State =
STATE_DISCONNECTING Next State = STATE_DEAD Current Substate = STATE_DISCONNECTING Next
Substate = STATE_DEAD
*Jul  2 13:33:24.851: sip_fsm:  FSM TYPE = SIP Timer-STate FSM, Event =
SIP_TIMER_REMOVE_TRANSACTION    Current State = STATE_DEAD
```

The following table describes the significant fields shown in the display.

Table 110: Command Field Name Descriptions

Field Name	Description
Called-Number	The destination number.
Calling-Number	The number that originated the call.
Sip-Call-Id	The SIP call ID.
Total Traces logged	The total number of traces logged for the specified message type.
buffer-id	The buffer ID uniquely identifies the buffer in which the traces are stored.

Field Name	Description
ccCallId	The call-id of the leg whose traces are displayed.
PeerCallId	The remote party call-id

show mrcp client session active

To display information about active Media Resource Control Protocol (MRCP) client sessions, use the **show mrcp client session active**command in privileged EXEC mode.

show mrcp client session active [**detailed**]

Syntax Description

detailed	(Optional) Displays detailed information about each active MRCP session.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.2(11)T	This command was introduced on the Cisco 3640, Cisco 3660, Cisco AS5300, Cisco AS5350, and Cisco AS5400.
12.4(15)T	The MRCP version, ASR callid, and TTS callid fields were added to the command output and the URL and Stream URL fields were modified to display Media Resource Control Protocol version 2 (MRCP v2) format URLs.

Usage Guidelines

Use this command to display information about all active MRCP sessions for the gateway. Use the **detailed** keyword to display additional information about the sessions.

Examples

The following is sample output from this command:

```
Router# show mrcp client session active
No Of Active MRCP Sessions:1
          Call-ID:0x1A
     Resource Type:Synthesizer        URL:rtsp://server-asr/synthesizer
Method In Progress:SPEAK      State:SPEAKING
     Resource Type:Recognizer         URL:rtsp://server-asr/recognizer
Method In Progress:RECOGNIZE      State:RECOGNIZING
```

The following is sample output when the **detailed** keyword is used:

```
Router# show mrcp client session active detailed
No Of Active MRCP Sessions: 1
           Call-ID: 0x14 same: 0
-------------------------------------------
     Resource Type: Synthesizer            URL: sip:mrcpv2TTSServer@10.5.18.224
Method In Progress: SPEAK                State: S_SYNTH_IDLE
Associated CallID: 0x17
     MRCP version: 2.0
 Control Protocol: TCP Server IP Address: 10.5.18.224    Port: 51000
    Data Protocol: RTP Server IP Address: 10.5.18.224    Port: 10000
Stream URL: sip:mrcpv2TTSServer@10.5.18.224:5060
Packets Transmitted: 0 (0 bytes)
Packets Received: 177 (28320 bytes)
ReceiveDelay: 100     LostPackets: 0
-------------------------------------------
-------------------------------------------
```

```
     Resource Type: Recognizer              URL: sip:mrcpv2ASRServer@10.5.18.224
Method In Progress: RECOGNITION-START-TIMERS             State: S_RECOG_RECOGNIZING
Associated CallID: 0x18
     MRCP version: 2.0
 Control Protocol: TCP Server IP Address: 10.5.18.224     Port: 51001
    Data Protocol: RTP Server IP Address: 10.5.18.224     Port: 10002
Packets Transmitted: 191 (30560 bytes)
Packets Received: 0 (0 bytes)
ReceiveDelay: 100     LostPackets: 0
```

The table below describes the fields shown in this output.

Table 111: show mrcp client session active detailed Field Descriptions

Field	Description
No. Of Active MRCP Sessions	Number of MRCP sessions that are currently active between the gateway and the media server.
Call-ID	Unique identification number for the call, in hexadecimal.
Resource Type	Whether the media server being used is a speech synthesizer (TTS) or a speech recognizer (ASR).
URL	URL of the media server.
Method In Progress	Type of event that was initiated between the gateway and the media server. Values are defined by the MRCP informational RFC. For speech synthesis, values are IDLE, SPEAK, SET-PARAMS, GET-PARAMS, STOP, or BARGE-IN-OCCURRED. For speech recognition, values are DEFINE-GRAMMAR, RECOGNIZE, SET-PARAMS, GET-PARAMS, STOP, GET-RESULT, or RECOGNITION-START-TIMERS.
State	Current state of the method in progress. Values are defined by the MRCP informational RFC. For speech synthesis, values are SYNTH_IDLE, SPEAKING, SYNTH_ASSOCIATING, PAUSED, or SYNTH_ERROR_STATE. For speech recognition, values are RECOG_IDLE, RECOG_ASSOCIATING, RECOGNIZING, RECOGNIZED, or RECOG_ERROR_STATE.
Associated CallID	Unique identification number for the associated MRCP session, in hexadecimal.
MRCP version	MRCP version used by the client.
Control Protocol	Call control protocol being used, which is always TCP.
Data Protocol	Data protocol being used, which is always RTP.
Local IP Address	IP address of the Cisco gateway that is the MRCP client. This field is not displayed for MRCP v2 sessions because the local IP address is not specified in SIP call legs.
Local Port	Identification number of the Cisco gateway port through which the TCP connection is made. This field is not displayed for MRCP v2 sessions because the local port is not specified in SIP call legs.

Field	Description
Server IP Address	IP address of the media server that is the MRCP server.
Server Port	Identification number of the MRCP server port through which the TCP connection is made.
Signalling URL	URL of the MRCP v2 media server.
Stream URL	URL of the MRCP v1 media server.
Packets Transmitted	Total number of packets that have been transmitted from the client to the ASR server.
Packets Received	Total number of packets that have been received by the client from the TTS server.
ReceiveDelay	Average playout FIFO delay plus the decoder delay during this voice call.

Related Commands

Command	Description
debug mrcp	Displays debug messages for MRCP operations.
show mrcp client session history	Displays information about past MRCP client sessions that are stored on the gateway.
show mrcp client statistics hostname	Displays statistics about MRCP sessions.

show mrcp client session history

To display information about past Media Resource Control Protocol (MRCP) client sessions that are stored on the gateway, use the **show mrcp client session history**command in privileged EXEC mode.

show mrcp client session history [**detailed**]

Syntax Description

detailed	(Optional) Displays detailed information about each MRCP session.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.2(11)T	This command was introduced on the Cisco 3640, Cisco 3660, Cisco AS5300, Cisco AS5350, and Cisco AS5400.
12.4(15)T	The MRCP version field was added to the command output and the URL field was modified to display Media Resource Control Protocol version 2 (MRCP v2) format URLs.

Usage Guidelines

The maximum number of inactive MRCP sessions that are stored in history is configured by using the **mrcp client session history records** command. If the **mrcp client session history records** command is not used, the maximum number of history records that are saved is 50.

MRCP history records are stored for the length of time that is specified by the **mrcp client session history duration** command. If the **mrcp client session history duration** command is not configured, MRCP history records are stored for a maximum of 3600 seconds (1 hour).

Examples

The following is sample output from this command:

```
Router# show mrcp client session history
MRCP Session ID:0x9
Associated CallID:0x1A
Control Protocol:TCP     Data Protocol:RTP
Local  IP Address:10.1.2.230     Local  Port 17120
Server IP Address:10.1.2.58     Server Port 4858
Stream URL:rtsp://server-asr:554
Packets Transmitted:423 (101520 bytes)
Packets Received:819 (131040 bytes)
MRCP Session ID:0x8
Associated CallID:0x16
Control Protocol:TCP     Data Protocol:RTP
Local  IP Address:10.1.2.230     Local  Port 16948
Server IP Address:10.1.2.58     Server Port 4850
Stream URL:rtsp://server-asr:554
Packets Transmitted:284 (68160 bytes)
Packets Received:598 (95680 bytes)
MRCP Session ID:0x7
Associated CallID:0x12
Control Protocol:TCP     Data Protocol:RTP
Local  IP Address:10.1.2.230     Local  Port 16686
Server IP Address:10.1.2.58     Server Port 4842
Stream URL:rtsp://server-asr:554
```

```
Packets Transmitted:353 (84720 bytes)
Packets Received:716 (114560 bytes)
MRCP Session ID:0x6
Associated CallID:0xE
Control Protocol:TCP     Data Protocol:RTP
Local  IP Address:10.1.2.230     Local  Port 19398
Server IP Address:10.1.2.58     Server Port 4834
Stream URL:rtsp://server-asr:554
Packets Transmitted:358 (85920 bytes)
Packets Received:720 (115200 bytes)
```

The following is sample output from the show mrcp client session history detailed command:

```
Router# show mrcp client session history detailed
MRCP Session ID: 0x7
Associated CallID: 0x14
     MRCP version: 2.0
     =================
     Control Protocol: TCP    Data Protocol: RTP
     ASR (Callid = 0x18)
Server IP Address: 10.5.18.224     Server Port 10002
Signalling URL: sip:mrcpv2ASRServer@10.5.18.224:5060
Packets Transmitted: 373 (59680 bytes)
Packets Received: 0 (0 bytes)
OntimeRcvPlayout: 3000
GapFillWithSilence: 0
GapFillWithPrediction: 0
GapFillWithInterpolation: 6025
GapFillWithRedundancy: 0
HighWaterPlayoutDelay: 100
LoWaterPlayoutDelay: 95
ReceiveDelay: 100     LostPackets: 0
EarlyPackets: 0     LatePackets: 0
----------------------------------------
     TTS (Callid = 0x17)
Server IP Address: 10.5.18.224     Server Port 10000
Signalling URL: sip:mrcpv2TTSServer@10.5.18.224:5060
Packets Transmitted: 0 (0 bytes)
Packets Received: 679 (108640 bytes)
OntimeRcvPlayout: 3000
GapFillWithSilence: 0
GapFillWithPrediction: 0
GapFillWithInterpolation: 6025
GapFillWithRedundancy: 0
HighWaterPlayoutDelay: 100
LoWaterPlayoutDelay: 95
ReceiveDelay: 100     LostPackets: 0
EarlyPackets: 0     LatePackets: 0
```

The table below describes the fields shown in this output.

Table 112: show mrcp client session history detailed Field Descriptions

Field	Description
MRCP Session ID	Unique identification number for the MRCP session, in hexadecimal.
Associated CallID	Unique identification number for the associated call, in hexadecimal.
MRCP version	MRCP version used by the client.
Control Protocol	Call control protocol being used, which is always TCP.

Field	Description
Data Protocol	Data protocol being used, which is always RTP.
ASR (Callid =)	For MRCP v2 sessions, the unique identification number for the ASR SIP call leg, in hexadecimal.
TTS (Callid =)	For MRCP v2 sessions, the unique identification number for the TTS SIP call leg, in hexadecimal.
Local IP Address	IP address of the Cisco gateway that is the MRCP client. This field is not displayed for MRCP v2 sessions because the local IP address is not specified in SIP call legs.
Local Port	Identification number of the Cisco gateway port through which the TCP connection is made. This field is not displayed for MRCP v2 sessions because the local port is not specified in SIP call legs.
Server IP Address	IP address of the media server that is the MRCP server.
Server Port	Identification number of the MRCP server port through which the TCP connection is made.
Signalling URL	URL of the MRCP v2 media server.
Stream URL	URL of the MRCP v1 media server.
Packets Transmitted	Total number of packets that have been transmitted from the client to the ASR server.
Packets Received	Total number of packets that have been received by the client from the TTS server.
OntimeRcvPlayout	Duration of voice playout from data received on time for this call. Derive the Total Voice Playout Duration for Active Voice by adding the OnTimeRcvPlayout value to the GapFill values.
GapFillWithSilence	Duration of a voice signal replaced with silence because voice data was lost or not received in time for this call.
GapFillWithPrediction	Duration of a voice signal played out with a signal synthesized from parameters or samples of data preceding in time because voice data was lost or not received in time from the voice gateway for this call. Examples of such pullout are frame-eraser or frame-concealment strategies in G.729 and G.723.1 compression algorithms.
GapFillWithInterpolation	Duration of a voice signal played out with a signal synthesized from parameters or samples of data preceding and following in time because voice data was lost or not received in time from the voice gateway for this call.
GapFillWithRedundancy	Duration of a voice signal played out with a signal synthesized from available redundancy parameters because voice data was lost or not received in time from the voice gateway for this call.
HighWaterPlayoutDelay	High-water mark voice playout FIFO delay during this call.

Field	Description
LoWaterPlayoutDelay	Low-water mark voice playout FIFO delay during this call.
ReceiveDelay	Average playout FIFO delay plus the decoder delay during this voice call.

Related Commands

Command	Description
debug mrcp	Displays debug messages for MRCP operations.
mrcp client session history duration	Sets the maximum number of seconds for which MRCP history records are stored on the gateway
mrcp client session history records	Sets the maximum number of MRCP history records that the gateway can store.
show mrcp client session active	Displays information about active MRCP client sessions.

show mrcp client statistics hostname

To display statistics about Media Resource Control Protocol (MRCP) sessions for a specific MRCP client host, use the **show mrcp client statistics hostname**command in privileged EXEC mode.

show mrcp client statistics hostname {*hostnameip-address*}

Syntax Description

hostname	Hostname of the MRCP server. Format uses host name only or hostname:port.
ip-address	IP address of the MRCP server.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.2(11)T	This command was introduced on the Cisco 3640, Cisco 3660, Cisco AS5300, Cisco AS5350, and Cisco AS5400.
12.4(15)T	This command was modified to display statistics about MRCP version 2 (MRCP v2) sessions.

Usage Guidelines

To display output from this command, you must first use the **mrcp client statistics enable**command.

Examples

The following is sample output from this command:

```
Router# show mrcp client statistics hostname asr-host
hostname:asr-host
Method                    :Count   Min   Avg   Max
RECOGNIZE                 :3       40    562   1604
DEFINE-GRAMMAR            :3       48    568   1604
RECOGNITION-START-TIMERS :2       140   164   188
SPEAK                     :6       44    568   1596
RECOG-TIME                :3       804   965   1128
SPEAK-TIME                :6       3636  7063  12068
```

The table below describes the fields shown in this output.

Table 113: show mrcp client statistics hostname Field Descriptions

Field	Description
hostname	Host name of the media server.
Method	Type of event that was initiated between the gateway and the media server. Values as defined by the MRCP informational RFC are RECOGNIZE, DEFINE-GRAMMAR, RECOGNITION-START-TIMERS, and SPEAK. RECOG-TIME is the milliseconds that it takes the ASR server to recognize the grammar. SPEAK-TIME is the milliseconds that it takes the TTS server to speak.
Count	Total number of MRCP sessions that used this method.

Field	Description
Min	Length of the shortest session, in milliseconds.
Avg	Average length of a session, in milliseconds, based on all sessions.
Max	Length of the longest session, in milliseconds.

Related Commands

Command	Description
debug mrcp	Displays debug messages for MRCP operations.
mrcp client statistics enable	Enables MRCP client statistics to be displayed.
show mrcp client session active	Displays information about active MRCP client sessions.
show mrcp client session history	Displays information about MRCP client history records that are stored on the gateway.

show mwi relay clients

To display registration information for the list of message-waiting indicator (MWI) relay clients, use the **show mwi relay clients**command in privileged EXEC mode.

show mwi relay clients

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.2(2)XT	This command was introduced on the Cisco 1750, Cisco 1751, Cisco 2600, Cisco 3600, and Cisco IAD2420.
12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T and implemented on the Cisco 3725 and Cisco 3745.
12.2(8)T1	This command was implemented on the Cisco 2600-XM and Cisco 2691.
12.2(11)T	This command was implemented on the Cisco 1760.

Examples

The following is sample output from thiscommand:

```
Router# show mwi relay clients
Client              IPADDR       EXPIRES(sec)  MWI
============  ===============  ============   ====
4085550153       10.8.17.25       89077        ON
6505550143       10.8.17.34       87654       OFF
```

The table below describes significant fields shown in this output.

Table 114: show mwi relay clients Field Descriptions

Field	Description
Client	Client number.
IPADDR	IP address.
EXPIRES	Seconds before expiration.
MWI	MWI status.

Related Commands

Command	Description
mwi relay	Enables the Cisco IOS Telephony Service router to relay MWI information to remote Cisco IP phones.

show nextport

To display statistical information on NextPort digital signal processor (DSP) resources for diagnostic and debugging purposes, use the **show nextport** command in privileged EXEC mode.

show nextport {**dfc** *slot/port* | **est** [*slot/dfc/module* | **enabled**] | **ifd** {**queue** *slot/port* [**control** | **data** | **est** | **gdb** | **voice** | *npaddress* [*qid*]] | **statistics**} | **md** *modem* | **mm** [*slot/dfc/module* | **interrupt**] | **np-address** *slot/port* | **session** {*slot/port* | **tty** *ttynumber*} | **siglib test** | **ssm** {**info** *slot/port* | **test** | **vdev** *slot/port*} | **test** | **vpd** {**statistics** *slot/port* | **traffic** *slot/port*} | **vsmgr protocol violations**}

Syntax Description

dfc *slot* / *port*	Displays dial feature card (DFC) manager statistics for the specified slot and port. Range for the slot and port numbers is 1 to 7. The slash is required in the command syntax.
est	Displays Error/Status/Trace (EST) statistics for all the NextPort modules.
est *slot* / *dfc* / *module*	Displays EST information for the NextPort module in the specified slot, DFC, and module location. The slash is required in the command syntax.
est enabled	Displays a list of the enabled NextPort modules.
ifd queue *slot* / *port*	Displays the contents of one or more NextPort interface driver queues for the specified slot and port. Information includes the contents of the free, ready, and index rings, and the buffer description tables. The slash is required in the command syntax.
control	(Optional) Displays statistics for the interface control driver queue.
data	(Optional) Displays statistics for the interface data driver queue.
est	(Optional) Displays statistics for the interface EST driver queue.
gdb	(Optional) Displays statistics for the interface GDB driver queue.
voice	(Optional) Displays statistics for the interface voice driver queue.
npaddress	(Optional) The module address, expressed as a number (for example, 0x06000100).
qid	(Optional) Specific queue ID number. Range is from 0 to 31.
ifd statistics	Displays interface driver statistics, including any weak assertions generated.
md *modem*	Displays information for the specified NextPort modem instance.
mm	Displays modem manager information for the enabled NextPort modules.
mm *slot* / *dfc* / *module*	Displays modem manager information for the specified slot, DFC, and module location. The slash is required in the command syntax.
mm interrupt	Displays a list of system timer interrupt enabled modules.

np-address *slot* / *port*	Displays the NextPort address for the specified slot and port. The slash is required in the command syntax.
session *slot* / *port*	Displays NextPort session information for the specified slot and port. The slash is required in the command syntax.
session tty *ttynumber*	Displays NextPort session information for the specified tty session. Range is from 0 to 2003.
siglib test	Displays statistics for the SigLib test configuration.
ssm info *slot* / *port*	Displays information about the NextPort session and service manager (SSM) for the specified slot and port. The slash is required in the command syntax.
ssm test	Displays svc_id type, service type, and signaling type for the unit test configuration.
ssm vdev *slot* / *port*	Displays NextPort SSM Vdev information for the specified slot and port. The slash is required in the command syntax.
test	Displays information about the NextPort test parameters configuration.
vpd statistics *slot* / *port*	Displays the TX/RX packet counters for voice packet drivers (VPDs) (including success and failure statistics). The *slot* / *port* argument limits the output to statistics for the specified slot and port. The slash is required in the command syntax.
vpd traffic *slot* / *port*	Displays TX/RX VPD traffic statistics for the specified slot and port. The slash is required in the command syntax.
vsmgr protocol violations	Displays the number of payload violations for the NextPort voice resource manager.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
15.1(2)T	Router output for the **show nextport mm**command updated.
12.1(1)XD1	The **show nextport ifd queue** command was introduced.
12.3(11)T	This command was modified. Keywords and arguments were added to expand the variations of command output. The command was renamed **show nextport** with the **ifd queue**keyword was added.

Usage Guidelines

The **show nextport** command is intended to be used by Cisco Technical Support personnel to look at the NextPort DSP statistics and to perform detailed debugging. Please consult Cisco Technical Support before using this command.

The **show nextport** command is supported on the Cisco AS5300XM series, Cisco AS5400XM series, and Cisco AS5800XM series platforms.

When you enter the **show nextport vpd statistics**command on the Cisco AS5850, the output shows the TX/RX packet counters that could not be forwarded by distributed Cisco Express Forwarding. These packets are routed back to the enhanced route switch controller (ERSC).

The **show nextport vpd statistics***slot*/*port* command (on individual feature boards) displays the TX/RX packet counts for the packets that have been forwarded by distributed Cisco Express Forwarding.

The display of packet counts for the packets forwarded on the Cisco AS5850 is the result of the distributed architecture of the platform.

Examples

The following examples show some of the variations of the **show nextport** command.



Note Field descriptions in the examples provided are self-explanatory.

```
Router# show nextport session 1/1
 Session Information Display
  slot/port : 1/1 TTY# : 217 Session ID : 0x006D
  Module Address : Slot 1 DFC 0 Module 0 SPE 0 Channel 1
  Service Type   : DATA FAX MODEM
  Session State  : IDLE
  TDM Information:
   DSP is connected to TDM stream 0, channel 1 on the NextPort module
Router# show nextport vpd statistics
Voice Statistics for slot 1
Status: Active
Rx Statistics
 rx_successful= 0
 rx_failed= 0
  queue destroyed = 0
  buffer pool depleted = 0
  invalid packet = 0
  wrong session packet = 0
  rejection by dsp api layer = 0
Tx Statistics
 tx_successful= 0
 tx_acked_by_ifd= 0
 tx_failed= 0
  rejection by IFD = 0
Voice Statistics for slot 2
Status: Idle
Rx Statistics
 rx_successful= 0
 rx_failed= 0
  queue destroyed = 0
  buffer pool depleted = 0
  invalid packet = 0
  wrong session packet = 0
  rejection by dsp api layer = 0
Tx Statistics
 tx_successful= 0
 tx_acked_by_ifd= 0
 tx_failed= 0
  rejection by IFD = 0
Voice Statistics for slot 3
Status: Active
Rx Statistics
 rx_successful= 0
 rx_failed= 0
```

```
  queue destroyed = 0
  buffer pool depleted = 0
  invalid packet = 0
  wrong session packet = 0
  rejection by dsp api layer = 0
Tx Statistics
 tx_successful= 0
 tx_acked_by_ifd= 0
 tx_failed= 0
  rejection by IFD = 0
Voice Statistics for slot 4
Status: Idle
Rx Statistics
 rx_successful= 0
 rx_failed= 0
  queue destroyed = 0
  buffer pool depleted = 0
  invalid packet = 0
  wrong session packet = 0
  rejection by dsp api layer = 0
Tx Statistics
 tx_successful= 0
 tx_acked_by_ifd= 0
 tx_failed= 0
  rejection by IFD = 0
Voice Statistics for slot 5
Status: Idle
Rx Statistics
 rx_successful= 0
 rx_failed= 0
  queue destroyed = 0
  buffer pool depleted = 0
  invalid packet = 0
  wrong session packet = 0
  rejection by dsp api layer = 0
Tx Statistics
 tx_successful= 0
 tx_acked_by_ifd= 0
 tx_failed= 0
  rejection by IFD = 0
Voice Statistics for slot 6
Status: Idle
Rx Statistics
 rx_successful= 0
 rx_failed= 0
  queue destroyed = 0
  buffer pool depleted = 0
  invalid packet = 0
  wrong session packet = 0
  rejection by dsp api layer = 0
Tx Statistics
 tx_successful= 0
 tx_acked_by_ifd= 0
 tx_failed= 0
  rejection by IFD = 0
Voice Statistics for slot 7
Status: Idle
Rx Statistics
 rx_successful= 0
 rx_failed= 0
  queue destroyed = 0
  buffer pool depleted = 0
  invalid packet = 0
  wrong session packet = 0
```

```
  rejection by dsp api layer = 0
Tx Statistics
 tx_successful= 0
 tx_acked_by_ifd= 0
 tx_failed= 0
  rejection by IFD = 0
Router# show nextport ssm vdev 3/1
vdev_common handle @ 0xC0D92E20
 slot 3, port 1, tone , device_status(0): VDEV_STATUS_UNLOCKED
csm_state(0x0100)=CSM_IDLE_STATE, csm_event_proc=0x601EA0C0
invalid_event_count=2, wdt_timeout_count=0
wdt_timestamp_started is not activated
wait_for_dialing:False, wait_for_bchan:False
pri_chnl=TDM_ISDN_STREAM(s0, u0, c0), tdm_chnl=TDM_DSP_STREAM(s3, c1)
dchan_idb_start_index=0, dchan_idb_index=0, call_id=0x0000, bchan_num=-1
csm_event=CSM_EVENT_MODEM_ONHOOK, cause=0x0007
ring_no_answer=0, ic_failure=0, ic_complete=0
dial_failure=0, oc_failure=0, oc_complete=0
oc_busy=0, oc_no_dial_tone=0, oc_dial_timeout=0
remote_link_disc=0, stat_busyout=0
oobp_failure=0, cas_address_signalling_failure=0
call_duration_started=00:00:00, call_duration_ended=00:00:00, total_call_durati0
The calling party phone number =
The called party phone number  =
total_free_rbs_timeslot = 0, total_busy_rbs_timeslot = 0, total_rtr_busy_rbs_ti,
total_sw56_rbs_timeslot = 0, total_sw56_rbs_static_bo_ts = 0,
total_free_isdn_channels = 0, total_auto_busy_isdn_channels = 0,
total_rtr_busy_isdn_channels = 0,
min_free_device_threshold = 0
Router# show nextport mm
IOS bundled NextPort image version: 0.0.0.0
NP Module(3 ): state = MODULE NOT INSERTED
IOS bundled NextPort image version: 0.0.0.0
NP Module(4 ): state = MODULE NOT INSERTED
IOS bundled NextPort image version: 0.0.0.0
NP Module(5 ): state = MODULE NOT INSERTED
IOS bundled NextPort image version: 0.0.0.0
NP Module(6 ): state = MODULE NOT INSERTED
IOS bundled NextPort image version: 0.0.0.0
NP Module(7 ): state = MODULE NOT INSERTED
IOS bundled NextPort image version: 0.0.0.0
NP Module(8 ): state = MODULE NOT INSERTED
IOS bundled NextPort image version: 0.0.0.0
NP Module(9 ): state = MODULE NOT INSERTED
IOS bundled NextPort image version: 0.0.0.0
NP Module(10): state = MODULE NOT INSERTED
IOS bundled NextPort image version: 0.0.0.0
NP Module(11): state = MODULE NOT INSERTED
IOS bundled NextPort image version: 7.37.10.90
NP Module(12): slot=4, dfc=0, module=0
               state = MODULE RUNNING
               crash=0, bad=0, restarts=0, num SPEs=6
               max_mpt_redundancy_session = 18
               spe country code = 0
               session handle enable = TRUE
IOS bundled NextPort image version: 7.37.10.90
NP Module(13): slot=4, dfc=0, module=1
               state = MODULE RUNNING
               crash=0, bad=0, restarts=0, num SPEs=6
               max_mpt_redundancy_session = 18
               spe country code = 0
               session handle enable = TRUE
IOS bundled NextPort image version: 7.37.10.90
NP Module(14): slot=4, dfc=0, module=2
```

```
                state = MODULE RUNNING
                crash=0, bad=0, restarts=0, num SPEs=6
                max_mpt_redundancy_session = 18
                spe country code = 0
                session handle enable = TRUE
IOS bundled NextPort image version: 7.37.10.90
NP Module(15): slot=5, dfc=0, module=0
                state = MODULE RUNNING
                crash=0, bad=0, restarts=0, num SPEs=6
                max_mpt_redundancy_session = 18
                spe country code = 0
                session handle enable = TRUE
IOS bundled NextPort image version: 7.37.10.90
NP Module(16): slot=5, dfc=0, module=1
                state = MODULE RUNNING
                crash=0, bad=0, restarts=0, num SPEs=6
                max_mpt_redundancy_session = 18
                spe country code = 0
                session handle enable = TRUE
IOS bundled NextPort image version: 7.37.10.90
NP Module(17): slot=5, dfc=0, module=2
                state = MODULE RUNNING
                crash=0, bad=0, restarts=0, num SPEs=6
                max_mpt_redundancy_session = 18
                spe country code = 0
                session handle enable = TRUE
IOS bundled NextPort image version: 0.0.0.0
NP Module(18): state = MODULE NOT INSERTED
IOS bundled NextPort image version: 0.0.0.0
NP Module(19): state = MODULE NOT INSERTED
IOS bundled NextPort image version: 0.0.0.0
NP Module(20): state = MODULE NOT INSERTED
IOS bundled NextPort image version: 0.0.0.0
NP Module(21): state = MODULE NOT INSERTED
IOS bundled NextPort image version: 0.0.0.0
NP Module(22): state = MODULE NOT INSERTED
IOS bundled NextPort image version: 0.0.0.0
NP Module(23): state = MODULE NOT INSERTED
```

Related Commands

Command	Description
show voice dsp	Displays the current status or selective statistics of DSP voice channels.

show nextport vpd

To display the TX/RX packet counters for voice packet drivers (VPDs) (including success and failure statistics), use the **show nextport vpd**command in privileged EXEC mode.

show nextport vpd {**statistics** [*slot*/*port-number*] | **traffic** [*slot*/*port-number*]}

Syntax Description

statistics	Displays information about the VPD statistics.
slot / *port number*	(Optional) The slot or port number of the interface.
traffic	Displays TX/RX VPD traffic statistics for the specified slot and port.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
15.0(1)M	This command was introduced in a release earlier than Cisco IOS Release 15.0(1)M.

Usage Guidelines

The **show nextport vpd statistics** command displays the TX/RX packet counters that could not be forwarded by distributed Cisco Express Forwarding (dCEF). These packets are routed back to the enhanced route switch controller (ERSC). Executing show nextport vpd statistics slot/port (on individual feature boards) shows the TX/RX packet counts for the packets that have been forwarded by dCEF.

Examples

The following is sample output from the **show nextport vpd traffic**command for slot1 ans port1:

```
Router# show nextport vpd traffic 1/1
Voice Instance for slot 1 port 1
Status: Idle
Session Duration in second: 0
Rx traffic Statistics
  total rx bytes: 0
  total rx packets: 0
  average rx packets per second: 0
Tx traffic Statistics
  total tx bytes: 0
  total tx packets: 0
  average tx packets per second: 0
```

The table below describes the significant fields shown in the display.

Table 115: show nextport vpd Field Descriptions

Field	Description
Status	Current status of the voice traffic.
Session	Duration of the voice sessions in seconds.
Rx traffic Statistics	Number of packets received.

Field	Description
Tx traffic Statistics	Number of packets sent.

The following is sample output from the **show nextport vpd statistics**command. The field descriptions are self-explanatory.

```
Router# show nextport vpd statistics
Voice Instance for slot 1 port 1
Status: Idle
Rx Statistics
  rx_successful= 0
  rx_failed= 0
    queue destroyed = 0
    buffer pool depleted = 0
    invalid packet = 0
    wrong session packet = 0
Tx Statistics
  tx_successful= 0
  tx_acked_by_ifd= 0
  tx_failed= 0
    rejection by IFD = 0
```

show num-exp

To display the number expansions configured, use the **show num-exp**command in privileged EXEC mode.

show num-exp [*dialed-number*]

Syntax Description

dialed -number	(Optional) Dialed number.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
11.3(1)T	This command was introduced on the Cisco 3600 series.
12.0(3)T	This command was implemented on the Cisco AS5300.
12.0(4)XL	This command was implemented on the Cisco AS5800.
12.0(7)XK	This command was implemented on the Cisco MC3810.
12.1(2)T	This command was integrated into Cisco IOS Release 12.1(2)T.

Usage Guidelines

Use this command to display all the number expansions configured for this router. To display number expansion for only one number, specify that number by using the *dialed-number* argument.

Examples

The following is sample output from this command:

```
Router# show num-exp
Dest Digit Pattern = '0...'     Translation = '+14085270...'
Dest Digit Pattern = '1...'     Translation = '+14085271...'
Dest Digit Pattern = '3..'      Translation = '+140852703..'
Dest Digit Pattern = '4..'      Translation = '+140852804..'
Dest Digit Pattern = '5..'      Translation = '+140852805..'
Dest Digit Pattern = '6....'    Translation = '+1408526....'
Dest Digit Pattern = '7....'    Translation = '+1408527....'
Dest Digit Pattern = '8...'     Translation = '+14085288...'
```

The table below describes significant fields shown in this output.

Table 116: show num-exp Field Descriptions

Field	Description
Dest Digit Pattern	Index number identifying the destination telephone number digit pattern.
Translation	Expanded destination telephone number digit pattern.

Related Commands

Command	Description
show call active voice	Displays the VoIP active call table.
show call history voice	Displays the VoIP call-history table.
show dial -peer voice	Displays configuration information for dial peers.
show voice port	Displays configuration information about a specific voice port.

show piafs status

To display the status of Personal Handyphone System (PHS) Internet Access Forum Standard (PIAFS) calls for each B channel in use on a router, use the **show piafs status** command in privileged EXEC mode.

show piafs status

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.2(8)T	This command was introduced on the Cisco 803, Cisco 804, and Cisco 813.

Examples

The following is sample output from this command showing the status of PIAFS calls on B channel 1 on a Cisco 813 router:

```
Router# show piafs status
PIAFS STATUS INFORMATION
------------------------
Number of active calls = 1
Details of connection 1
**********************
Call Direction is: INCOMING
Call speed is: 64K
Current speed is: 64K
Call Elapsed Time: 59 seconds
The B channel assigned for this call is: B1 CHAN
Control Parameters Agreed Upon:
ARQ Control Information Transfer Protocol: Version 1
ARQ Data Transmission Protocol: Version 1
Measured RTF value: 9
PIAFS Frame Length in Bytes: 80
Maximum Frame Number: 63
Data Transmission Protocol of Peer: FIXED SPEED
Data Transmission Protocol of 800 Router: FIXED SPEED
V42 Negotiated: YES
V42 Parameters:
Direction: BOTH
No of code words: 4096
Max string length: 250
First PPP Frame Detected: YES
Piafs main FSM state: PIAFS_DATA
PIAFS Data Frames Tx Statistics:
Total No: of PIAFS Frames Confirmed: 344
Total Bytes of Application Data Transmitted:
Before Compression:  47021
After Compression: 30952
Compression Ratio in Tx direction is 1.51: 1
Total No: of PIAFS Frames Retransmitted: 32
Total Bytes of Application Data Retransmitted: 2336
Total Throughput in Tx Direction:
Including PIAFS Dummy Frames: 8000 Bytes/Second
Excluding PIAFS Dummy Frames: 859 Bytes/Second
```

```
Excluding PIAFS Dummy and Retransmitted Data Frames: 593 Bytes/Second
PIAFS Data Frames Rx Statistics:
Total No: of PIAFS Frames Received: 86
Total No: of Bad PIAFS Frames Received: 0
Total Bytes of Application Data Received:
Before Uncompression: 1459
After Uncompression: 2955
Compression Ratio in Rx direction is 2.02: 1
Total Throughput in Rx Direction:
Including PIAFS Dummy Frames: 8000 Bytes/Second
Excluding PIAFS Dummy Frames: 656 Bytes/Second
Excluding PIAFS Dummy and Retransmitted Data Frames: 126 Bytes/Second
No: of ReSynchronizations so far: 0
```

The table below describes significant fields shown in this output.

Table 117: show piafs status Field Descriptions

Field	Description
First PPP Frame Detected	If the output shows "YES," the first PPP frame from the peer device has been detected by the Cisco 803, Cisco 804, or Cisco 813 router. If the output shows "NO," the router has not received any PPP frames from the peer device.
Piafs main FSM state	Valid states for the finite state machine (FSM) are Initialization, Sync, Control, and Data.

Related Commands

Command	Description
debug piafs events	Displays debugging messages for PIAFS calls.

show platform hardware qfp active feature sbc fork global

To display media forking statistics that are related to all the forking instances for an active Cisco Quantum Flow Processor (QFP) instance of CUBE, use the **show platform hardware qfp active feature sbc fork global** command in privileged EXEC mode.

show platform hardware qfp active feature sbc fork global

Syntax Description

qfp	Cisco Quantum Flow Processor (QFP).
active	Displays the active instance of the processor.
sbc	Session Border Controller. CUBE is a Session Border Controller.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Bengaluru 17.6.1a	This command was modified to include statistics that are related to Websocket-based media forking.
Cisco IOS Release 15.2(1)S	This command was introduced.

Usage Guidelines

Use this command to display the global media forking statistics related to all the media forking instances of a CUBE platform. Media forking statistics that are related to WebSocket connections are included in the command as part of Cisco IOS XE Bengaluru 17.6.1a release. The statistics that are displayed for WebSocket-based media forking includes **SBC WebSocket Fork Global Statistics**, **Dropped RTP Packets**, and **Dropped Control Packets**. The section **SBC WebSocket Fork Global Statistics** displays statistics that are related to the transmission (TX) and receipt (RX) of RTP packets. For instance, the drop and replication of RTP packets in a media forking scenario. It also includes statistical details on the forward and drop of packets to control the session parameters in WebSocket-based media forking. The section **Dropped RTP Packets** provides statistical insight into the reasons for RTP packet drop. **Dropped Control Packets** contains statistical insight into the reasons for control packet drop.

Examples

The following sample output displays the media forking statistics, related to a CUBE platform:

```
router#show platform hardware qfp active feature sbc fork global
SBC Media Fork Global Statistics
------------------------------

  Total TX RTP packets replicated            = 0
  Total TX RTP octets replicated             = 0
  Total TX RTP packets dropped               = 0
  Total TX RTP octets dropped                = 0
  Total RX RTP packets replicated            = 0
  Total RX RTP octets replicated             = 0
  Total RX RTP packets dropped               = 0
  Total RX RTP octets dropped                = 0

SBC WebSocket Fork Global Statistics
------------------------------
```

```
Total TX RTP packets replicated             = 23641
Total TX RTP octets replicated              = 5413789
Total TX RTP packets dropped                = 0
Total TX RTP octets dropped                 = 0
Total RX RTP packets replicated             = 23641
Total RX RTP octets replicated              = 5413789
Total RX RTP packets dropped                = 0
Total RX RTP octets dropped                 = 0
Total control packets forwarded             = 6
Total control octets forwarded              = 1662
Total control packets dropped               = 0
Total control octets dropped                = 0

Dropped RTP Packets
----------------------------

  Without associated fork session           = 0
  Invalid socket connection                 = 0
  Invalid stream ID                         = 0
  Invalid packet data                       = 0
  WebSocket frame build failure             = 0
  Protobuf encoding failure                 = 0
  Socket write failure                      = 0
  TLS sb setup failure                      = 0
  TLS encryption failure                    = 0
  Internal error                            = 0

Dropped Control Packets
----------------------------

  Without associated fork session           = 0
  Invalid socket connection                 = 0
  Invalid packet data                       = 0
  WebSocket frame decode failure            = 0
  Invalid WebSocket frame                   = 0
  Socket write failure                      = 0
  TLS sb setup failure                      = 0
  TLS encryption failure                    = 0
  Internal error                            = 0
```

Related Commands

Command	Description
show voip stream-service connection history	Displays information about all the closed WebSocket connections in CUBE.
show voip stream-service server <ip:port>	Displays information about the WebSocket connection that is based on the WebSocket server IP and port.
show voip stream-service connection id <id>	Displays information about a WebSocket connection that is based on the WebSocket ID. Also, it displays all the forked call details.

show platform hardware qfp active feature sbc fork session

To display media forking statistics specific to a fork session for an active Cisco Quantum Flow Processor (QFP) instance of CUBE, use the **show platform hardware qfp active feature sbc fork session***id* command in privileged EXEC mode.

show platform hardware qfp active feature sbc fork session *id*

Syntax Description

qfp	Cisco Quantum Flow Processor (QFP).
active	Displays the active instance of the processor.
sbc	Session Border Controller. CUBE is a Session Border Controller.
id	The ID associated with a WebSocket media forking session.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Bengaluru 17.6.1a	This command was modified to include statistics that are related to Websocket-based media forking.
Cisco IOS Release 15.2(1)S	This command was introduced.

Usage Guidelines

Use this command to display the statistics related to a specific media forking session in a WebSocket connection. The statistical information is displayed for the active instance of the QFP. The statistics that are displayed for WebSocket-based media forking as part of this command includes the following categories:

- **SBC WebSocket Fork Session Information**
  - **Primary call mgm correlator** and **Primary call mpf correlator**—Displays information that is related to the correlators of the original call.
  - **RX stream ID** and **TX stream ID**—Displays information about the WebSocket channels that are used to perform forking.
  - **Primary call anchor side**—Displays information about the side of the anchor on the call that is associated with the forking session.
  - **Payload type**—Displays information about the payload encoding type or the payload type that is contained in the packets. For example, payload type is zero for G711ulaw and eight for G711alaw.
- **SBC WebSocket Connection Information**—The forking session is associated with a WebSocket connection. Displays information about the WebSocket connection that is related to your forking session. This section contains information on whether your WebSocket connection is secure or not. Also, it provides information on the Local IP and port, Remote IP and port, WebSocket ID and WebSocket TCP socket ID.

- **SBC WebSocket Fork Session Statistics**—Displays information about the RTP packet drop and packet replication for both TX and RX streams. Also, it provides information on the packet drop and packet forward count for control packets.

Examples

The following sample output displays the media forking statistics, related to a fork session in a WebSocket connection:

```
router#show platform hardware qfp active feature sbc fork session 1
SBC WebSocket Fork Session Information
--------------------------------------

  Fork session ID                              = 1
  Fork session mgm correlator                  = 2
  Primary call mgm correlator                  = 1
  Primary call mpf correlator                  = 1
  Primary call anchor side                     = SIDE_A
  RX stream ID                                 = 1
  TX stream ID                                 = 2
  Payload type                                 = 0

SBC WebSocket Connection Information
--------------------------------------

  Secure                                       = No
  WebSocket ID                                 = 3
  WebSocket TCP socket ID                      = 0xec5f26c0
  Local port                                   = 38122
  Local IP (if v4)                             = 0a40565b
  Local IP (if v6)                             = 0a40565b:00000000:00000000:00000000
  Remote port                                  = 8083
  Remote IP (if v4)                            = 0a4056d7
  Remote IP (if v6)                            = 0a4056d7:00000000:00000000:00000000

SBC WebSocket Fork Session Statistics
--------------------------------------

  Total TX RTP packets replicated              = 3073
  Total TX RTP octets replicated               = 491680
  Total TX RTP packets dropped                 = 174
  Total TX RTP octets dropped                  = 30972
  Total RX RTP packets replicated              = 3071
  Total RX RTP octets replicated               = 491360
  Total RX RTP packets dropped                 = 176
  Total RX RTP octets dropped                  = 31328
  Total control packets forwarded              = 2
  Total control octets forwarded               = 464
  Total control packets dropped                = 0
  Total control octets dropped                 = 0
```

Related Commands

Command	Description
show voip stream-service connection history	Displays information about all the closed WebSocket connections in CUBE.
show voip stream-service server <ip:port>	Displays information about the WebSocket connection that is based on WebSocket server IP and port address.

Command	Description
show voip stream-service connection id <id>	Displays information about a WebSocket connection that is based on the WebSocket ID. Also, it displays all the forked call details.

show pots csm

To display the current state of calls and the most recent event received by the call-switching module (CSM) on a Cisco 800 series router, use the **show pots csm** command in privileged EXEC mode.

show pots csm *port*

Syntax Description

port	Port number. Range is from 1 to 2.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.1.(2)XF	This command was introduced on the Cisco 800 series.

Examples

The following is sample output from this command:

```
Router# show pots csm 1
POTS PORT: 1
   CSM Finite State Machine:
      Call 0 - State: idle, Call Id: 0x0
               Active: no
               Event: CSM_EVENT_NONE Cause: 0
      Call 1 - State: idle, Call Id: 0x0
               Active: no
               Event: CSM_EVENT_NONE Cause: 0
      Call 2 - State: idle, Call Id: 0x0
               Active: no
               Event: CSM_EVENT_NONE Cause: 0
```

Field descriptions should be self-explanatory.

Related Commands

Command	Description
test pots dial	Dials a telephone number for the POTS port on the router by using a dial application on your workstation.
test pots disconnect	Disconnects a telephone call for the POTS port on the router.

show pots status

To display the settings of the telephone port physical characteristics and other information on the telephone interfaces of a Cisco 800 series router, use the **show pots status**command in privileged EXEC mode.

show pots status [**1** | **2**]

Syntax Description

1	(Optional) Displays the settings of telephone port 1.
2	(Optional) Displays the settings of telephone port 2.

Command Default

No default behavior or values

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.0(3)T	This command was introduced on the Cisco 800 series.

Examples

The following is sample output from thiscommand.

```
Router# show pots status
POTS Global Configuration:
   Country: United States
   Dialing Method: Overlap, Tone Source: Remote, CallerId Support: YES
   Line Type: 600 ohm, PCM Encoding: u-law, Disc Type: OSI,
   Ringing Frequency: 20Hz, Distinctive Ring Guard timer: 0 msec
   Disconnect timer: 1000 msec, Disconnect Silence timer: 5 sec
   TX Gain: 6dB, RX Loss: -6dB,
   Filter Mask: 6F
   Adaptive Cntrl Mask: 0
POTS PORT: 1
   Hook Switch Finite State Machine:
      State: On Hook, Event: 0
      Hook Switch Register: 10, Suspend Poll: 0
   CODEC Finite State Machine:
      State: Idle, Event: 0
      Connection: None, Call Type: Two Party, Direction: Rx only
      Line Type: 600 ohm, PCM Encoding: u-law, Disc Type: OSI,
      Ringing Frequency: 20Hz, Distinctive Ring Guard timer: 0 msec
      Disconnect timer: 1000 msec, Disconnect Silence timer: 5 sec
      TX Gain: 6dB, RX Loss: -6dB,
      Filter Mask: 6F
      Adaptive Cntrl Mask: 0
   CODEC Registers:
      SPI Addr: 2, DSLAC Revision: 4
      SLIC Cmd: 0D, TX TS: 00, RX TS: 00
      Op Fn: 6F, Op Fn2: 00, Op Cond: 00
      AISN: 6D, ELT: B5, EPG: 32 52 00 00
      SLIC Pin Direction: 1F
   CODEC Coefficients:
      GX: A0 00
      GR: 3A A1
```

```
       Z: EA 23 2A 35 A5 9F C2 AD 3A AE 22 46 C2 F0
       B: 29 FA 8F 2A CB A9 23 92 2B 49 F5 37 1D 01
       X: AB 40 3B 9F A8 7E 22 97 36 A6 2A AE
       R: 01 11 01 90 01 90 01 90 01 90 01 90
      GZ: 60
     ADAPT B: 91 B2 8F 62 31
   CSM Finite State Machine:
      Call 0 - State: idle, Call Id: 0x0
               Active: no
      Call 1 - State: idle, Call Id: 0x0
               Active: no
      Call 2 - State: idle, Call Id: 0x0
               Active: no
POTS PORT: 2
   Hook Switch Finite State Machine:
      State: On Hook, Event: 0
      Hook Switch Register: 20, Suspend Poll: 0
   CODEC Finite State Machine:
      State: Idle, Event: 0
      Connection: None, Call Type: Two Party, Direction: Rx only
      Line Type: 600 ohm, PCM Encoding: u-law, Disc Type: OSI,
      Ringing Frequency: 20Hz, Distinctive Ring Guard timer: 0 msec
      Disconnect timer: 1000 msec, Disconnect Silence timer: 5 sec
      TX Gain: 6dB, RX Loss: -6dB,
      Filter Mask: 6F
      Adaptive Cntrl Mask: 0
   CODEC Registers:
      SPI Addr: 3, DSLAC Revision: 4
      SLIC Cmd: 0D, TX TS: 00, RX TS: 00
      Op Fn: 6F, Op Fn2: 00, Op Cond: 00
      AISN: 6D, ELT: B5, EPG: 32 52 00 00
      SLIC Pin Direction: 1F
   CODEC Coefficients:
      GX: A0 00
      GR: 3A A1
       Z: EA 23 2A 35 A5 9F C2 AD 3A AE 22 46 C2 F0
       B: 29 FA 8F 2A CB A9 23 92 2B 49 F5 37 1D 01
       X: AB 40 3B 9F A8 7E 22 97 36 A6 2A AE
       R: 01 11 01 90 01 90 01 90 01 90 01 90
      GZ: 60
     ADAPT B: 91 B2 8F 62 31
   CSM Finite State Machine:
      Call 0 - State: idle, Call Id: 0x0
               Active: no
      Call 1 - State: idle, Call Id: 0x0
               Active: no
      Call 2 - State: idle, Call Id: 0x0
               Active: no
Time Slot Control: 0
```

The table below describes significant fields shown in this output.

Table 118: show pots status Field Descriptions

Field	Descriptions
POTS Global Configuration	Settings of the telephone port physical characteristic commands. Also displays the following: • TX GAIN--Current transmit gain of telephone ports. • RX LOSS--Current transmit loss of telephone ports. • Filter Mask--Value determines which filters are currently enabled or disabled in the telephone port hardware. • Adaptive Cntrl Mask--Value determines if telephone port adaptive line impedance hardware is enabled or disabled.
Hook Switch Finite State Machine	Device driver that tracks state of telephone port hook switch.
CODEC Finite State Machine	Device driver that controls telephone port codec hardware.
CODEC Registers	Register contents of telephone port codec hardware.
CODEC Coefficients	Codec coefficients selected by telephone port driver. Selected line type determines codec coefficients.
CSM Finite State Machine	State of call-switching module (CSM) software.
Time Slot Control	Register that determines if telephone port voice or data packets are sent to an ISDN B channel.

Related Commands

Command	Description
pots country	Configures telephones, fax machines, or modems connected to a Cisco 800 series router to use country-specific default settings for each physical characteristic.
pots dialing-method	Specifies how the Cisco 800 series router collects and sends digits dialed on your connected telephones, fax machines, or modems.
pots disconnect-supervision	Specifies how a Cisco 800 series router notifies the connected telephones, fax machines, or modems when the calling party has disconnected.
pots disconnect-time	Specifies the interval in which the disconnect method is applied if telephones, fax machines, or modems connected to a Cisco 800 series router fail to detect that a calling party has disconnected.
pots distinctive-ring-guard-time	Specifies a delay in which a telephone port can be rung after a previous call is disconnected (Cisco 800 series routers).
pots encoding	Specifies the PCM encoding scheme for telephones, fax machines, or modems connected to a Cisco 800 series router.

Command	Description
pots line-type	Specifies the impedance of telephones, fax machines, or modems connected to a Cisco 800 series router.
pots ringing-freq	Specifies the frequency at which telephones, fax machines, or modems connected to a Cisco 800 series router ring.
pots silence-time	Specifies the interval of silence after a calling party disconnects (Cisco 800 series router).
pots tone-source	Specifies the source of dial, ringback, and busy tones for telephones, fax machines, or modems connected to a Cisco 800 series router.

show pots volume

To display the receiver volume level that is configured for each POTS port on a router, use the **show pots volume** command in privileged EXEC mode.

show pots volume

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.2(8)T	This command was introduced on the Cisco 803, Cisco 804, and Cisco 813.

Examples

The following is sample output from this command showing that the receiver volume level is 5 for both POTS port 1 and POTS port 2.

```
Router# show pots volume
POTS PORT 1: Volume 5
POTS PORT 2: Volume 5
```

Field descriptions should be self-explanatory.

Related Commands

Command	Description
volume	Configures the receiver volume level for a POTS port on a router.

show presence global

To display configuration information about the presence service, use the **show presence global** command in user EXEC or privileged EXEC mode.

show presence global

Syntax Description

This command has no arguments or keywords.

Command Modes

User EXEC (>)
Privileged EXEC (#)

Command History

Release	Modification
12.4(11)XJ	This command was introduced.
12.4(15)T	This command was integrated into Cisco IOS Release 12.4(15)T.

Usage Guidelines

This command displays the configuration settings for presence.

Examples

The following example displays output from the **show subscription global** command:

```
Router# show subscription global
Presence Global Configuration Information:
==========================================
Presence feature enable            : TRUE
Presence allow external watchers   : FALSE
Presence max subscription allowed  : 100
Presence number of subscriptions   : 0
Presence allow external subscribe  : FALSE
Presence call list enable          : TRUE
Presence server IP address         : 0.0.0.0
Presence sccp blfsd retry interval : 60
Presence sccp blfsd retry limit    : 10
Presence router mode               : CME mode
```

The table below describes the significant fields shown in the display.

Table 119: show subscription global Field Descriptions

Field	Description
Presence feature enable	Indicates whether presence is enabled on the router with the **presence** command.
Presence allow external watchers	Indicates whether internal presentities can be watched by external watchers, as set by the **watcher all** command
Presence max subscription allowed	Maximum number of presence subscriptions allowed by the **max-subscription** command.

Field	Description
Presence number of subscriptions	Current number of active presence subscriptions.
Presence allow external subscribe	Indicates whether internal watchers are allowed to subscribe to status notifications from external presentities, as set by the **allow subscribe** command.
Presence call list enable	Indicates whether the Busy Lamp Field (BLF) call-list feature is enabled with the **presence call-list** command.
Presence server IP address	Displays the IP address of an external presence server defined with the **server** command.
Presence sccp blfsd retry interval	Retry timeout, in seconds, for BLF speed-dial numbers on SCCP phones set by the **sccp blf-speed-dial retry interval** command.
Presence sccp blfsd retry limit	Maximum number of retries allowed for BLF speed-dial numbers on SCCP phones set by the **sccp blf-speed-dial retry interval** command.
Presence router mode	Indicates whether the configuration mode is set to Cisco Unified CME or Cisco Unified SRST by the **mode** command.

Related Commands

Command	Description
allow watch	Allows a directory number on a phone registered to Cisco Unified CME to be watched in a presence service.
allow subscribe	Allows internal watchers to monitor external presence entities (directory numbers).
debug presence	Displays debugging information about the presence service.
presence enable	Allows the router to accept incoming presence requests.
server	Specifies the IP address of a presence server for sending presence requests from internal watchers to external presence entities.
show presence subscription	Displays information about active presence subscriptions.
watcher all	Allows external watchers to monitor internal presence entities (directory numbers).

show presence subscription

To display information about active presence subscriptions, use the **show presence subscription** command in user EXEC or privileged EXEC mode.

show presence subscription [**details** | **presentity** *telephone-number* | **subid** *subscription-id* | **summary**]

Syntax Description

details	(Optional) Displays detailed information about presentities, watchers, and presence subscriptions.
presentity *telephone-number*	(Optional) Displays information on the presentity specified by the destination telephone number.
subid *subscription-id*	(Optional) Displays information for the specific subscription ID.
summary	(Optional) Displays summary information about active subscription requests.

Command Default

Information for all active presence subscriptions is displayed.

Command Modes

User EXEC (>)
Privileged EXEC (#)

Command History

Release	Modification
12.4(11)XJ	This command was introduced.
12.4(15)T	This command was integrated into Cisco IOS Release 12.4(15)T.
12.4(24)T	This command was integrated into Cisco IOS Release 12.4(24)T.

Usage Guidelines

This command displays details about the currently active presence subscriptions

Examples

The following is sample output from the **show presence subscription details** command:

```
Presence Active Subscription Records Details:
=============================================

Subscription ID         : 1
  Watcher               : 6002@10.4.171.60
  Presentity            : 6005@10.4.171.34
  Expires               : 3600 seconds
  Subscription Duration : 1751 seconds
  line status           : idle
  watcher type          : local
  presentity type       : local
  Watcher phone type    : SIP Phone
  subscription type     : Incoming Indication
  retry limit           : 0
  sibling subID         : 0
  sdb                   : 0
```

```
  dp                    : 6555346C
  watcher dial peer tag : 40001
  number of presentity  : 1

Subscription ID         : 2
  Watcher               : 6002@10.4.171.60

Presence Active Subscription Records:
=============================================

Subscription ID         : 30
  Watcher               : 4085550103@10.4.171.34
  Presentity            : 5001@10.4.171.20
  Expires               : 3600 seconds
  line status           : idle
  watcher type          : local
  presentity type       : remote
  Watcher phone type    : SCCP [BLF Call List]
  subscription type     : Outgoing Request
  retry limit           : 0
  sibling subID         : 23
  sdb                   : 0
  dp                    : 0
  watcher dial peer tag : 0
```

The following is sample output from the **show presence subscription summary** command:

```
Router# show presence subscription summary

Presence Active Subscription Records Summary: 15 subscription
Watcher                 Presentity              SubID  Expires SibID  Status
======================= ======================= ====== ======= ====== ======
6002@10.4.171.60        6005@10.4.171.34         1     3600    0      idle
6005@10.4.171.81        6002@10.4.171.34         6     3600    0      idle
6005@10.4.171.81        6003@10.4.171.34         8     3600    0      idle
6005@10.4.171.81        6002@10.4.171.34         9     3600    0      idle
6005@10.4.171.81        6003@10.4.171.34         10    3600    0      idle
6005@10.4.171.81        6001@10.4.171.34         12    3600    0      idle
6001@10.4.171.61        6003@10.4.171.34         15    3600    0      idle
6001@10.4.171.61        6002@10.4.171.34         17    3600    0      idle
6003@10.4.171.59        6003@10.4.171.34         19    3600    0      idle
6003@10.4.171.59        6002@10.4.171.34         21    3600    0      idle
6003@10.4.171.59        5001@10.4.171.34         23    3600    24     idle
6002@10.4.171.60        6003@10.4.171.34         121   3600    0      idle
6002@10.4.171.60        5002@10.4.171.34         128   3600    129    idle
6005@10.4.171.81        1001@10.4.171.34         130   3600    131    busy
6005@10.4.171.81        7005@10.4.171.34         132   3600    133    idle
```

The following is sample output from the **show presence subscription summary** command showing that device-based BLF monitoring is enabled on two phones.

```
Watcher                  Presentity              SubID  Expires SibID  Status
======================== ======================= ====== ======= ====== ======
D 2036@10.6.2.6          2038@10.6.2.254          33     3600    0      idle

  2036@10.6.2.6          2038@10.6.2.254          35     3600    0      idle

D 2036@10.6.2.6          8883@10.6.2.254          37     3600    0      unknown
```

The following is sample output from the **show presence subscription subid**command:

```
Router# show presence subscription subid 133

Presence Active Subscription Records:
=============================================

Subscription ID         : 133
  Watcher               : 6005@10.4.171.34
  Presentity            : 7005@10.4.171.20
  Expires               : 3600 seconds
  line status           : idle
  watcher type          : local
  presentity type       : remote
  Watcher phone type    : SIP Phone
  subscription type     : Outgoing Request
  retry limit           : 0
  sibling subID         : 132
  sdb                   : 0
  dp                    : 0
  watcher dial peer tag : 0
```

The table below describes the significant fields shown in the display.

Table 120: show presence subscription Field Descriptions

Field	Description
Watcher	IP address of the watcher.
Presentity	IP address of the presentity.
Expires	Number of seconds until the subscription expires. Default is 3600.
line status	Status of the line: • Idle--Line is not being used. • In-use--User is on the line, whether or not this line can accept a new call. • Unknown--Phone is unregistered or this line is not allowed to be watched.
watcher type	Whether the watcher is local or remote.
presentity type	Whether the presentity is local or remote.
Watcher phone type	Type of phone, either SCCP or SIP.
subscription type	The type of presence subscription, either incoming or outgoing.
retry limit	Maximum number of times the router attempts to subscribe for the line status of an external SCCP phone when either the presentity does not exist or the router receives a terminated NOTIFY from the external presence server. Set with the **sccp blf-speed-dial retry-interval** command.
sibling subID	Sibling subscription ID if presentity is remote. If value is 0, presentity is local.
sdb	Voice port of the presentity.

Field	Description
dp	Dial peer of the presentity.
watcher dial peer tag	Dial peer tag of the watcher device.

Related Commands

Command	Description
allow watch	Allows a directory number on a phone registered to Cisco Unified CME to be watched in a presence service.
blf-speed-dial	Enables BLF monitoring for a speed-dial number on a phone registered to Cisco Unified CME.
debug ephone blf	Displays debugging information for BLF presence features.
debug presence	Displays debugging information about the presence service.
presence	Enables presence service and enters presence configuration mode.
presence enable	Allows the router to accept incoming presence requests.
show presence global	Displays configuration information about the presence service.

show proxy h323 calls

To display a list of active calls on the proxy, use the **show proxy h323 calls** command in privilegedEXEC mode.

show proxy h323 calls

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
11.3(2)NA	This command was introduced.
12.0(3)T	The command was integrated into Cisco IOS Release 12.0(3)T and implemented on the Cisco MC3810.

Examples

The following is sample output from thiscommand:

```
Router# show proxy h323 calls
Call unique key = 1
  Conference ID = [277B87C0A283D111B63E00609704D8EA]
  Calling endpoint call signalling address = 55.0.0.41
  Calling endpoint aliases:
   H323_ID: ptel11@zone1.com
  Call state = Media Streaming
  Time call was initiated = 731146290 ms
```

Field descriptions should be self-explanatory.

Related Commands

Command	Description
show proxy h323 detail-call	Displays the details of a particular call on a proxy.
show proxy h323 status	Displays the overall status of a proxy.

show proxy h323 detail-call

To display the details of a particular call on a proxy, use the **show proxy h323 detail-call** command in privileged EXEC mode.

show proxy h323 detail-call *call-key*

Syntax Description

call -key	Call to be displayed, derived from the **show proxy h323 calls** command output.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
11.3(2)NA	This command was introduced.
12.0(3)T	The command was integrated into Cisco IOS Release 12.0(3)T and implemented on the Cisco MC3810.

Usage Guidelines

You can use this command with or without proxy statistics enabled.

Examples

The following is sample output from this command without proxy statistics enabled:

```
Router# show proxy h323 detail-call 1
ConferenceID = [277B87C0A283D111B63E00609704D8EA]
Calling endpoint aliases:
      H323_ID: ptel11@zone1.com
Called endpoint aliases:
      H323_ID: ptel21@zone2.com
Peer proxy call signalling address = 172.17.0.41
Time call was initiated = 731146290 ms
Inbound CRV = 144
Outbound CRV = 70
Call state = Media Streaming
H245 logical channels for call leg pte111@zone1.com<->px1@zone.com
    Channel number = 2
        Type = VIDEO
        State = OPEN
        Bandwidth = 374 kbps
        Time created = 731146317 ms
    Channel number = 1
        Type = AUDIO
        State = OPEN
        Bandwidth = 81 kbps
        Time created = 731146316 ms
    Channel number = 2
        Type = VIDEO
        State = OPEN
        Bandwidth = 374 kbps
        Time created = 731146318 ms
    Channel number = 1
        Type = AUDIO
        State = OPEN
        Bandwidth = 81 kbps
```

```
        Time created = 731146317 ms
H245 logical channels for call leg pte111@zone1.com<->172.17.50.21:
    Channel number = 2
        Type = VIDEO
        State = OPEN
        Bandwidth = 374 kbps
        Time created = 731146317 ms
    Channel number = 1
        Type = AUDIO
        State = OPEN
        Bandwidth = 81 kbps
        Time created = 731146316 ms
    Channel number = 2
        Type = VIDEO
        State = OPEN
        Bandwidth = 374 kbps
        Time created = 731146318 ms
    Channel number = 1
        Type = AUDIO
        State = OPEN
        Bandwidth = 81 kbps
        Time created = 731146317 ms
```

The following is sample output from this command with proxy statistics enabled:

```
Router# show proxy h323 detail-call 1
ConferenceID = [677EB106BD0D111976200002424F832]
Calling endpoint call signalling address = 172.21.127.49
    Calling endpoint aliases:
      H323_ID: intel2
      E164_ID: 2134
Called endpoint aliases:
      H323_ID: mcs@sanjose.cisco.com
Peer proxy call signalling address = 172.68.183.199
Peer proxy aliases:
      H323_ID: proxy.sanjose.cisco.com
Time call was initiated = 730949651 ms
Inbound CRV = 2505
Outbound CRV = 67
Call state = H245 open logical channels
H245 logical channels for call leg intel2 <-> cisco7-pxy:
    Channel number = 259
      RTP stream from intel2 to cisco7-pxy
        Type = VIDEO
        State = OPEN
        Bandwidth = 225 kbps
        Time created = 730949676 ms
    Channel number = 257
      RTP stream from intel2 to cisco7-pxy
        Type = AUDIO
        State = OPEN
        Bandwidth = 18 kbps
        Time created = 730949658 ms
    Channel number = 2
      RTP stream from cisco7-pxy to intel2
        Type = VIDEO
        State = OPEN
        Bandwidth = 225 kbps
        Time created = 730949664 ms
        RTP Statistics:
          Packet Received Count = 3390
          Packet Dropped Count = 0
          Packet Out of Sequence Count = 0
          Number of initial packets used for Arrival-Spacing bin setup = 200
```

```
min_arrival_spacing = 0(ms)  max_arrival_spacing = 856(ms)
Average Arrival Rate = 86(ms)
Arrival-Spacing(ms)   Packet-Count
   0                     2116
   26                    487
   52                    26
   78                    0
   104                   0
   130                   1
   156                   0
   182                   1
   208                   0
   234                   4
   260                   99
   286                   315
   312                   154
   338                   8
   364                   0
   390                   2
   416                   10
   442                   73
   468                   51
   494                   43
==============================
Min Jitter = 34(ms)  Max Jitter = 408(ms)
Average Jitter Rate = 117
Jitter Rate(ms)   Packet-Count
   0                     0
   41                    514
   82                    2117
Number of initial packets used for Arrival-Spacing bin setup = 200
min_arrival_spacing = 32(ms)  max_arrival_spacing = 96(ms)
Average Arrival Rate = 60(ms)
Arrival-Spacing(ms)   Packet-Count
   32                    35
   34                    0
   36                    177
   38                    0
   40                    56
   42                     0
   44                    10
   46                    0
   48                    27
   50                    0
   52                    541
   54                    0
   56                    2642
   58                    1
   60                    1069
   62                    0
   64                    77 0
   68                    6
   70                    257
==============================
Min Jitter = 0(ms)  Max Jitter = 28(ms)
Average Jitter Rate = 5
Jitter Rate(ms)   Packet-Count
   0                     1069
   3                     2720
   6                     0
   9                     804
   12                    27
   15                    10
   18                    0
```

```
            21                    56
            24                    177
            27                    35
H245 logical channels for call leg cisco7-pxy <->
proxy.sanjose.cisco.com:
    Channel number = 259
      RTP stream from cisco7-pxy to proxy.sanjose.cisco.com
        Type = VIDEO
        State = OPEN
        Bandwidth = 225 kbps
        Time created = 730949676 ms
        RTP Statistics:
          Packet Received Count = 3398
          Packet Dropped Count = 1
          Packet Out of Sequence Count = 0
          Number of initial packets used for Arrival-Spacing bin setup = 200
          min_arrival_spacing = 0(ms)  max_arrival_spacing = 872(ms)
          Average Arrival Rate = 85(ms)
          Arrival-Spacing(ms)   Packet-Count
             0                     2636
             28                    0
             56                    0
             84                    0
             112                   0
             140                   1
             168                   0
             196                   0
             224                   0
             252                   0
             280                   2
             308                   425
             336                   154
             364                   5
             392                   0
             420                   0
             448                   0
             476                   114
             504                   41
             532                   20
          ==============================
          Min Jitter = 55(ms)  Max Jitter = 447(ms)
          Average Jitter Rate = 127
          Jitter Rate(ms)   Packet-Count
             0                     0
             45                    1
             90                    2636
             135                   0
             180                   2
             225                   425
             270                   159
             315                   0
             360                   0
             405                   175
    Channel number = 257
      RTP stream from cisco7-pxy to proxy.sanjose.cisco.com
        Type = AUDIO
        State = OPEN
        Bandwidth = 18 kbps
        Time created = 730949658 ms
        RTP Statistics:
          Packet Received Count = 2537
          Packet Dropped Count = 3
          Packet Out of Sequence Count = 0
          Number of initial packets used for Arrival-Spacing bin setup = 200
```

```
        min_arrival_spacing = 0(ms)  max_arrival_spacing = 32716(ms)
        Average Arrival Rate = 112(ms)
        Arrival-Spacing(ms)   Packet-Count
           0                     2191
           72                    253
           144                   31
           216                   7
           288                   3
           360                   4
           432                   4
           504                   2
           576                   1
           648                   3
           720                   2
           792                   1
           864                   2
           936                   1
           1008                  1
           1080                  1
           1152                  1
           1224                  1
           1296                  0
           1368                  28
        ============================
        Min Jitter = 32(ms)  Max Jitter = 1256(ms)
        Average Jitter Rate = 121
        Jitter Rate(ms)   Packet-Count
           0                     284
           126                   2201
           252                   4
           378                   6
           504                   4
           630                   3
           756                   2
           882                   2
           1008                  2
           1134                  29
    Channel number = 2
      RTP stream from proxy.sanjose.cisco.com to cisco7-pxy
        Type = VIDEO
        State = OPEN
        Bandwidth = 225 kbps
        Time created = 730949664 ms
    Channel number = 1
      RTP stream from proxy.sanjose.cisco.com to cisco7-pxy
        Type = AUDIO
        State = OPEN
        Bandwidth = 18 kbps
        Time created = 730949661 ms
```

Field descriptions should be self-explanatory.

Related Commands

Command	Description
h323 qos	Enables QoS on the proxy.
show proxy h323 calls	Displays a list of active calls on the proxy.
show proxy h323 status	Displays the overall status of a proxy.

show proxy h323 status

To display the overall status of a proxy, use the **show proxy h323 status**command in privileged EXEC mode.

show proxy h323 status

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
11.3(2)NA	This command was introduced.
12.0(3)T	The command was integrated into Cisco IOS Release 12.0(3)T and implemented on the Cisco MC3810.

Examples

The following is sample output from this command:

```
Router# show proxy h323 status
  H.323 Proxy Status
        ==================
    H.323 Proxy Mode: Enabled
    Proxy interface = Serial1: UP
    Application Specific Routing: Disabled
    RAS Initialization: Complete
    Proxy aliases configured:
      H323_ID: px2
    Proxy aliases assigned by Gatekeeper:
      H323_ID: px2
    Gatekeeper multicast discovery: Disabled
    Gatekeeper:
        Gatekeeper ID: gk.zone2.com
        IP address: 70.0.0.31
    Gatekeeper registration succeeded
    T.120 Mode: BYPASS
    RTP Statistics: OFF
    Number of calls in progress: 1
```

Field descriptions should be self-explanatory.

Related Commands

Command	Description
show proxy h323 calls	Displays a list of active calls on the proxy.
show proxy h323 detail-call	Displays the details of a particular call on a proxy.

show raw

To display leaking raw buffers that have been captured, use the **show raw** command in privileged EXEC mode.

show raw {**all** | **cas** | **ccapi** | **h323** | **ivr** | **reclaimed** | **tsp** | **vtsp**}

Syntax Description

all	Displays the record of all sections.
cas	Displays the record of channel-associated signaling (CAS).
ccapi	Displays the application programming interface (API) that is used to coordinate interaction between application and call legs (telephony or IP).
h323	Displays the record of the H.323 subsystem.
ivr	Displays the record of interactive voice response (IVR).
reclaimed	Displays the raw buffers reclaimed by the audit module.
tsp	Displays the telephony service provider (TSP) subsystem.
vtsp	Displays the voice telephony service provider (VTSP) subsystem.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.2(2)XU3	This command was introduced.
12.2(11)T	This command was integrated into Cisco IOS Release 12.2(11)T.

Usage Guidelines

The number of raw leaks that are displayed by the **show raw reclaimed** command should be zero, indicating that there are no memory leaks.

Examples

The following is a sample output from this command showing that there are no leaking raw buffers:

```
Router# show raw reclaimed
RAW LEAK REPORT:
ORPHAN : 0 raw buffers reclaimed
TSP : 0 raw buffers reclaimed
VTSP : 0 raw buffers reclaimed
H323 : 0 raw buffers reclaimed
SIP : 0 raw buffers reclaimed
CCAPI : 0 raw buffers reclaimed
```

VOATM : 0 raw buffers reclaimed

XGCP : 0 raw buffers reclaimed

CAS : 0 raw buffers reclaimed

IVR : 0 raw buffers reclaimed

SSAPP : 0 raw buffers reclaimed

Last Audit Session is at 20:28:13 UTC Fri Mar 27 2002

The table below describes significant fields shown in this output.

Table 121: show raw reclaimed Field Descriptions

Field	Description
ORPHAN	R aw buffers when a valid owner is not found.
TSP	Raw buffers on the telephony service provider (TSP) subsystem.
VTSP	Raw buffers on the voice telephony service provider (VTSP) subsystem.
H323	Raw buffers on the H.323 subsystem.
SIP	Raw buffers on the Session Initiation Protocol session.
CCAPI	Raw buffers on the API system used to coordinate interaction between application and call legs (telephony or IP).
VOATM	Raw buffers on the Voice over ATM network.
XGCP	Raw buffers on external media gateway control protocols. Includes Simple Gateway Control Protocol (SGCP) and Media Gateway Control Protocol (MGCP).
CAS	Raw buffers on the channel-associated signaling (CAS).
IVR	Raw buffers on the interactive voice response (IVR) system.
SSAPP	Raw buffers on the session application.

Related Commands

Command	Description
show rawmsg	Shows raw messages owned by the required component.

show rawmsg

To display the raw messages owned by the required component, use the **show rawmsg** command in privileged EXEC mode.

show rawmsg {**all** | **cas** | **ccapi** | **h323** | **ivr** | **reclaimed** | **tsp** | **vtsp**}

Syntax Description

all	Displays the raw messages owned by all the components.
cas	Displays the Channel Associated Signaling (CAS) subsystem.
ccapi	Displays the Application programming interface (API) used to coordinate interaction between application and call legs (telephony or IP).
h323	Displays the H.323 subsystem.
ivr	Displays the Interactive Voice Response (IVR) subsystem.
reclaimed	Displays the raw reclaimed by the audit module.
tsp	Displays the Telephony Service Provider (TSP) subsystem.
vtsp	Displays the Voice Telephony Service Provider (VTSP) subsystem.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.0(7)T	This command was introduced on the Cisco AS5300.
12.4(24)T	This command was modified in a release earlier than Cisco IOS Release 12.4(24)T. The **cas**, **ivr**, and **reclaimed** keywords were added.

Usage Guidelines

The number displayed for the **show rawmsg all** command should be zero to indicate that there are no memory leaks.

Examples

The following is a sample output from the **show rawmsg tsp** command that displays memory leaks from the Telephony Service Provider. The field names are self-explanatory.

```
Router# show rawmsg tsp
 Raw Msg Summary:
       Raw Msg in used: 0
```

Related Commands

Command	Description
isdn protocol-emulate	Configures the Layer 2 and Layer 3 port protocol of a BRI voice port or a PRI interface to emulate NT (network) or TE (user) functionality.

Command	Description
isdn switch type	Configures the Cisco AS5300 PRI interface to support Q.SIG signaling.
pri-group nec-fusion	Configures the NEC PBX to support FCCS.
show cdapi	Displays the CDAPI.

show rlm group statistics

To display the network latency of a Redundant Link Manager (RLM) group, use the **show rlm group statistics**command in privileged EXEC mode.

show rlm group [*group-number*] **statistics**

Syntax Description

group -number	(Optional) RLM group number. The range is from 0 to 255. There is no default value.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
11.3(7)	This command was introduced.
12.4(22)T	This command was integrated into Cisco IOS Release 12.4(22)T.

Usage Guidelines

You can specify the *group-number* argument to view the network latency of a specific RLM group. If you do not specify the *group-number* argument, then the **show rlm group statistics** command displays the network latency of all the configured RLM groups.

Examples

The following is sample output from the **show rlm group statistics** command:

```
Router# show rlm group statistics
RLM Group Statistics
 Link_up:
     last time occurred at 02:45:48.724, total transition=1
     avg=00:00:00.000, max=00:00:00.000, min=00:00:00.000, latest=00:00:00.000
 Link_down:
     last time occurred at 02:42:33.724, total transition=1
     avg=00:03:15.000, max=00:03:15.000, min=00:00:00.000, latest=00:03:15.000
 Link_recovered:
     last time occurred at 00:00:00.000, success=0(0%), failure=0
     avg=0.000s, max=0.000s, min=0.000s, latest=0.000s
 Link_switched:
     last time occurred at 00:00:00.000, success=0(0%), failure=0
     avg=0.000s, max=0.000s, min=0.000s, latest=0.000s
 Server_changed:
     last time occurred at 00:00:00.000 for totally 0 times
 Server Link Group[r1-server]:
  Open the link [10.1.1.1(Loopback1), 10.1.4.1]:
     last time occurred at 02:43:03.724, success=1(100%), failure=0
     avg=162.000s, max=162.000s, min=0.000s, latest=162.000s
  Echo over link [10.1.1.1(Loopback1), 10.1.4.1]:
     last time occurred at 02:47:15.724, success=91(62%), failure=54
     avg=0.000s, max=0.000s, min=0.000s, latest=0.000s
  Open the link [10.1.1.2(Loopback2), 10.1.4.2]:
     last time occurred at 02:43:03.724, success=1(100%), failure=0
     avg=162.000s, max=162.000s, min=0.000s, latest=162.000s
  Echo over link [10.1.1.2(Loopback2), 10.1.4.2]:
     last time occurred at 02:47:19.724, success=95(63%), failure=54
     avg=0.000s, max=0.000s, min=0.000s, latest=0.000s
 Server Link Group[r2-server]:
```

```
  Open the link [10.1.1.1(Loopback1), 10.1.5.1]:
     last time occurred at 02:46:06.724, success=0(0%), failure=1
     avg=0.000s, max=0.000s, min=0.000s, latest=0.000s
  Echo over link [10.1.1.1(Loopback1), 10.1.5.1]:
     last time occurred at 02:47:18.724, success=0(0%), failure=85
     avg=0.000s, max=0.000s, min=0.000s, latest=0.000s
Open the link [10.1.1.2(Loopback2), 10.1.5.2]:
     last time occurred at 02:46:06.724, success=0(0%), failure=1
     avg=0.000s, max=0.000s, min=0.000s, latest=0.000s
  Echo over link [10.1.1.2(Loopback2), 10.1.5.2]:
     last time occurred at 02:47:18.724, success=0(0%), failure=85
     avg=0.000s, max=0.000s, min=0.000s, latest=0.000s
```

The table below describes the significant fields shown in the display.

Table 122: show rlm group statistics Field Descriptions

Field	Description
Link_up	Statistics collected when the RLM group is in the link up state.
total transition	Total number of transitions into a particular RLM group state.
avg	Total average time (in seconds) that the interval lasts.
max	Total maximum time (in seconds) that the interval lasts.
min	Total minimum time (in seconds) that the interval lasts.
latest	The most recent interval.
Link_down	Statistics collected when the RLM group is in the link down state.
Link_recovered	Statistics collected when the RLM group is in the link recovery state.
Link_switched	Statistics collected when the RLM group is in the link switching state.
Server_changed	Statistics collected for when and how many times an RLM server failover happens.
Server Link Group[r1-server]	Statistics collected for the signaling links defined under a particular server link group, for example, r1-server.
Open the link	Statistics collected when a particular signaling link connection is open (broken).
Echo over link	Statistics collected when a particular signaling link connection is established.

Related Commands

Command	Description
clear interface	Resets the hardware logic on an interface.
clear rlm group	Clears all RLM group time stamps to zero.
interface	Configures an interface type and enters interface configuration mode.
link (RLM)	Specifies the link preference.

Command	Description
protocol rlm port	Reconfigures the port number for the basic RLM connection for the whole RLM group.
retry keepalive	Allows consecutive keepalive failures a certain amount of time before the link is declared down.
server (RLM)	Defines the IP address of the server.
show rlm group status	Displays the status of an RLM group.
show rlm group timer	Displays the current RLM group timer values.
shutdown (RLM)	Shuts down all of the links under an RLM group.
timer	Overwrites the default setting of timeout values.

show rlm group status

To display the status of a Redundant Link Manager (RLM) group, use the **show rlm group status** command in privileged EXEC mode.

show rlm group [*group-number*] **status**

Syntax Description

group -number	(Optional) RLM group number. The range is from 0 to 255. There is no default value.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
11.3(7)	This command was introduced.
12.4(22)T	This command was integrated into Cisco IOS Release 12.4(22)T.

Usage Guidelines

You can specify the *group-number* argument to view the status of a specific RLM group. If you do not specify the *group-number* argument, then the **show rlm group status** command displays the status of all the configured RLM groups.

Examples

The following is sample output from the **show rlm group status** command:

```
Router# show rlm group status
RLM Group 1 Status
 User/Port: RLM_MGR/3000
 Link State: Up          Last Link Status Reported: Up
 Next tx TID: 1          Last rx TID: 0
 Server Link Group[r1-server]:
  link [10.1.1.1(Loopback1), 10.1.4.1] = socket[active]
  link [10.1.1.2(Loopback2), 10.1.4.2] = socket[standby]
 Server Link Group[r2-server]:
  link [10.1.1.1(Loopback1), 10.1.5.1] = socket[opening]
  link [10.1.1.2(Loopback2), 10.1.5.2] = socket[opening]
```

The table below describes the significant fields shown in the display.

Table 123: show rlm group status Field Descriptions

Field	Description
User/Port	List of registered RLM users and the port numbers associated with them.
RLM_MGR	RLM management module.
Link State	Current RLM group's link state for connecting to the remote end.
Last Link Status Reported	Most recent link status change is reported to RLM users.
Next tx TID	Next transaction ID for transmission.

Field	Description
Last rx TID	Most recent transaction ID has been received.
Server Link Group[r1-server]	Status of all signaling links configured under a particular RLM server link group, for example, r1-server.
socket	Status of the individual signaling link.

Related Commands

Command	Description
clear interface	Resets the hardware logic on an interface.
clear rlm group	Clears all RLM group time stamps to zero.
interface	Configures an interface type and enters interface configuration mode.
link (RLM)	Specifies the link preference.
protocol rlm port	Reconfigures the port number for the basic RLM connection for the whole RLM group.
retry keepalive	Allows consecutive keepalive failures a certain amount of time before the link is declared down.
server (RLM)	Defines the IP address of the server.
show rlm group statistics	Displays the network latency of an RLM group.
show rlm group timer	Displays the current RLM group timer values.
shutdown (RLM)	Shuts down all of the links under an RLM group.
timer	Overwrites the default setting of timeout values.

show rlm group timer

To display the current timer values of a Redundant Link Manager (RLM) group, use the **show rlm group timer** command in privileged EXEC mode.

show rlm group [*group-number*] **timer**

Syntax Description

group -number	(Optional) RLM group number. The range is from 0 to 255. There is no default value.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
11.3(7)	This command was introduced.
12.4(22)T	This command was integrated into Cisco IOS Release 12.4(22)T.

Usage Guidelines

You can specify the *group-number* argument to view the timer values of a specific RLM group. If you do not specify the *group-number* argument, then the **show rlm group timer**command displays the timer values of all the configured RLM groups.

Examples

The following is sample output from the **show rlm group timer** command:

```
Router# show rlm group timer
RLM Group 1 Timer Values
 open_wait  = 3s                force-down  = 30s
 recovery   = 12s               switch-link = 5s
 minimum-up = 60s               retransmit  = 1s
 keepalive  = 1s
```

The table below describes the significant fields shown in the display.

Table 124: show rlm group timer Field Descriptions

Field	Description
open_wait	Wait for the connection request to be acknowledged.
recovery	Time (in seconds) to allow the link to recover to backup link before declaring the link is down.
minimum-up	Minimum time (in seconds) to force RLM to stay in the link down state for the remote end to detect that the link state is down.
keepalive	A keepalive packet is sent out from the network access server to the Card Security Code (CSC) periodically.
force-down	Minimum time (in seconds) to force RLM to stay in the link down state for the remote end to detect that the link state is down.

Field	Description
switch-link	The maximum transition period allows RLM to switch from a lower preference link to a higher preference link. If the switching link does not complete successfully before this timer expires, RLM goes into the recovery state.
retransmit	Because RLM is operating under User Datagram Protocol (UDP), it needs to resend the control packet if the packet is not acknowledged within this retransmit interval (in seconds).

Related Commands

Command	Description
clear interface	Resets the hardware logic on an interface.
clear rlm group	Clears all RLM group time stamps to zero.
interface	Configures an interface type and enters interface configuration mode.
link (RLM)	Specifies the link preference.
protocol rlm port	Reconfigures the port number for the basic RLM connection for the whole RLM group.
retry keepalive	Allows consecutive keepalive failures a certain amount of time before the link is declared down.
server (RLM)	Defines the IP address of the server.
show rlm group statistics	Displays the network latency of an RLM group.
show rlm group status	Displays the status of an RLM group.
shutdown (RLM)	Shuts down all of the links under an RLM group.
timer	Overwrites the default setting of timeout values.

show rpms-proc counters

To display statistics for the number of leg 3 authentication, authorization, and accounting (AAA) preauthentication requests, successes, and rejects, use the **show rpms-proc counters** command in privileged EXEC mode.

show rpms-proc counters

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.2(11)T	This command was introduced.

Usage Guidelines

Leg 3 refers to a call segment from the IP network to a terminating (outgoing) gateway that takes traffic from an IP network to a PSTN network.

Examples

The following sample output displays leg 3 statistics for AAA preauthentication requests, successes, and rejects:

```
Router# show rpms-proc counters
H323 Calls
Preauth Requests Sent      : 43433
Preauth Requests Accepted  : 43433
Preauth Requests Rejected  : 0
Preauth Requests TimedOut  : 0
Disconnects during Preauth : 0
SIP Calls
Preauth Requests Sent      : 43080
Preauth Requests Accepted  : 43080
Preauth Requests Rejected  : 0
Preauth Requests TimedOut  : 0
Disconnects during Preauth : 0
```

The table below describes significant fields shown in this output.

Table 125: show rpms-proc counters Field Descriptions

Field	Description
Preauth Requests Sent	Number of preauthentication requests sent.
Preauth Requests Accepted	Number of preauthentication requests accepted.
Preauth Requests Rejected	Number of preauthentication requests rejected.
Preauth Requests Timed Out	Number of preauthentication requests rejected because they timed out.
Disconnects during Preauth	Number of calls that were disconnected during the preauthentication process.

Related Commands

Command	Description
clear rpms -proc counters	Clears statistics counters for AAA preauthentication requests, successes, and rejects.

show running-config dial-peer

To display only dial-peer configuration information from running configuration, use the **show running-config dial-peer** command in privileged EXEC (#) mode.

show running-config dial-peer {**sort** [**descending**] | **voice** *tag*}

Command Default

None

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
15.5(2)T, Cisco IOS XE Release 3.15S	This command was introduced.

Usage Guidelines

The **show running-config dial-peer** command displays the dial-peers in the running-configuration based on the timestamp in which they were configured.

Example

In the below examples, 5, 4020, and 5000 indicate dial-peer tags. The following command displays the dial-peers in ascending order of timestamp in which they were configured:

```
Device# show running-config dial-peer

dial-peer voice 4020 pots
 destination-pattern 4020
 port 0/2/0
!
dial-peer voice 5000 voip
 destination-pattern 5...
 session protocol sipv2
 session target ipv4:1.4.65.5
!
dial-peer voice 5 pots
incoming called-number 1...
port 1/0/0:23
```

The following command displays the dial-peers in ascending order of dial-peer tag:

```
Device# show running-config dial-peer sort

dial-peer voice 5 pots
incoming called-number 1...
port 1/0/0:23
!
dial-peer voice 4020 pots
 destination-pattern 4020
 port 0/2/0
!
dial-peer voice 5000 voip
 destination-pattern 5...
 session protocol sipv2
 session target ipv4:1.4.65.5
```

The following command displays the dial-peers in descending order of dial-peer tag:

```
Device# show running-config dial-peer sort descending

dial-peer voice 5000 voip
 destination-pattern 5...
 session protocol sipv2
 session target ipv4:1.4.65.5
!
dial-peer voice 4020 pots
 destination-pattern 4020
 port 0/2/0
!
dial-peer voice 5 pots
incoming called-number 1...
port 1/0/0:23
```

The following command displays the dial-peer information specific to a dial-peer tag:

```
Device# show running-config dial-peer voice 4020

dial-peer voice 4020 pots
 destination-pattern 4020
 port 0/2/0
```

show rtpspi

To display Real-time Transport Protocol (RTP) serial peripheral interface (SPI) active call details and call statistics, use the **show rtpspi**command in privileged EXEC mode.

show rtpspi {**call** | **statistics**}

Syntax Description

call	Displays RTP SPI active call details.
statistics	Displays RTP SPI call statistics information.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.4(22)T	This command was introduced in a release earlier than Cisco IOS Release 12.4(22)T.

Examples

The following is sample output from the **show rtpspi statistics**command:

```
Router# show rtpspi statistics
RTP Statistics info:
No. CallId     Xmit-pkts Xmit-bytes Rcvd-pkts  Rcvd-bytes Lost pkts  Jitter Latenc
1   48         0x3BA     0x25440    0x17       0xD99      0x0        0x0      0x0
2   50         0x3BA     0x4A88     0x70       0x8AD      0x0        0x0      0x0
```

The table below describes the significant fields shown in the display.

Table 126: show rtpspi statistics Field Descriptions

Field	Description
CallId	The call ID number.
Xmit-pkts	Number of packets transmitted.
Xmit-bytes	Number of bytes transmitted.
Rcvd-pkts	Number of packets received.
Rcvd-bytes	Number of bytes received.
Lost pkts	Number of lost packets.
Jitter	Reports the jitter encountered.
Latenc	Reports the level of latency on the call.

Related Commands

Command	Description
debug rtpspi all	Debugs all RTP SPI errors, sessions, and in/out functions.

show rtsp client session

To display cumulative information about Real Time Streaming Protocol (RTSP) session records, use the **show rtsp client session** command in privileged EXEC mode.

show rtsp client session {**history** | **active**} [**detailed**]

Syntax Description

history	Displays cumulative information about the session, packet statistics, and general call information such as call ID, session ID, individual RTSP stream URLs, packet statistics, and play duration.
active	Displays session and stream information for the stream that is currently active.
detailed	(Optional) Displays session and stream information in detail for all streams that are associated with the session. This keyword is not available on Cisco 7200 series routers.

Command Default

Active (current) stream information is displayed.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.1(3)T	This command was introduced on the Cisco AS5300.
12.1(5)T	This command was implemented on the Cisco AS5800.
12.1(5)XM2	This command was implemented on the Cisco AS5350 and Cisco AS5400.
12.2(2)XB1	This command was implemented on the Cisco AS5850.
12.2(4)XM	This command was implemented on the Cisco 1750 and Cisco 1751. Support for the Cisco AS5300, Cisco AS5350, Cisco AS5400, Cisco AS5800 and Cisco AS5850 is not included in this release.
12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T and implemented on the Cisco 7200 series. This command is supported on the Cisco AS5300, Cisco AS5350, Cisco AS5400, Cisco AS5800, and Cisco AS5850 in this release.

Usage Guidelines

Use this command to display cumulative information about the session, packet statistics, and general call information such as call ID and session ID.



Note Session refers to a session between the application and the RTSP client. Each call leg that is configured to use RTSP streaming has a session.

A call leg could play several prompts in a session; the "Play Time" refers to the play time associated with a stream or, in other words, a prompt; the cumulative play time is the sum total of all streams (or prompts) played out in a session.

The command output is a stream block that contains information about the stream (URL, packet statistics, current state of the stream, play duration, call ID, session ID, individual RTSP stream URLs, and packet statistics).

Examples

The following is sample output from the **show rtsp client session active** command :

```
Router# show rtsp client session active
RTSP Session ID:0x8     Current Status:RTSP_STATUS_PLAYING
Associated CallID:0xF
Active Request:RTSP_API_REQ_PLAY
Control Protocol:TCP     Data Protocol:RTP
Total Packets Transmitted:0 (0 bytes)
Total Packets Received:708 (226560 bytes)
Cumulative Elapsed Play   Time:00:00:28.296
Cumulative Elapsed Record Time:00:00:00.000
        Session ID:0x8     State:ACTIVE
        Local  IP Address:10.13.79.45     Local  Port 16660
        Server IP Address:10.13.79.6     Server Port 11046
        Stream URL:rtsp://rtsp-cisco.cisco.com:554/chinna.au/streamid=0
        Packets Transmitted:0 (0 bytes)
        Packets Received:708 (226560 bytes)
        Elapsed Play   Time:00:00:28.296
        Elapsed  Record Time:00:00:00.000
        ReceiveDelay:85     LostPackets:0
```

The following is sample output from the **show rtsp client session history detailed** command:

```
Router# show rtsp client session history detailed
RTSP Session ID:0x8
Associated CallID:0xF
Control Protocol:TCP     Data Protocol:RTP
Total Packets Transmitted:0 (0 bytes)
Total Packets Received:2398 (767360 bytes)
Cumulative Elapsed Play   Time:00:01:35.916
Cumulative Elapsed Record Time:00:00:00.000
        Session ID:0x8     State:INACTIVE
        Local  IP Address:10.13.79.45     Local  Port 16660
        Server IP Address:10.13.79.6     Server Port 11046
        Stream URL:rtsp://rtsp-cisco.cisco.com:554/chinna.au/streamid=0
        Packets Transmitted:0 (0 bytes)
        Packets Received:2398 (767360 bytes)
        Play   Time:00:01:35.916
        Record Time:00:00:00.000
        OntimeRcvPlayout:93650
        GapFillWithSilence:0
        GapFillWithPrediction:70
        GapFillWithInterpolation:0
        GapFillWithRedundancy:0
        HighWaterPlayoutDelay:85
        LoWaterPlayoutDelay:64
        ReceiveDelay:85     LostPackets:0
        EarlyPackets:2     LatePackets:12
```

The table below describes significant fields shown in this output.

Table 127: show rtsp client session Field Descriptions

Field	Description
RTSP Session ID:0x8	Unique ID for the RTSP session.

Field	Description
Current Status:RTSP_STATUS_PLAYING	Current status: • RTSP_STATUS_SESSION_IDLE • RTSP_STATUS_SERVER_CONNECTED • RTSP_STATUS_PLAY_PAUSED • RTSP_STATUS_PLAY_COMPLETE
Associated CallID:0xF	ID of associated call.
Control Protocol:TCP	Transport protocol.
Data Protocol:RTP	Data protocol.
Total Packets Transmitted:0 (0 bytes)	Bytes sent out to the RTSP server.
Total Packets Received:708 (226560 bytes)	Bytes received from the server for playing.

Related Commands

Command	Description
rtsp client session history duration	Specifies the length of time for which the RTSP is kept during the session.
rtsp client session history records	Specifies the number of RTSP client session history records during the session.

show rudpv0 failures

To display SS7 Reliable User Datagram Protocol (RUDP) failure statistics, use the **show rudpv0 failures** command in privileged EXEC mode.

show rudpv0 failures

Syntax Description

This command has no keywords or arguments.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.0(7)XR	This command was introduced.
12.1(1)T	This command was integrated into Cisco IOS Release 12.1(1)T.

Examples

The following is sample output from this command showing displaying RUDP failures.

```
Router# show rudpv0 failures
**** RUDP Failure Stats ****
CreateBufHdrsFailure       0
CreateConnRecsFailure      0
CreateEventsFailure        0
NotReadyFailures           0
OptionNotSupportedFailures 0
OptionRequiredFailures     0
GetConnRecFailures         0
InvalidConnFailures        0
EventUnavailFailures       0
EmptyBufferSendFailures    0
BufferTooLargeFailures     0
ConnNotOpenFailures        0
SendWindowFullFailures     0
GetBufHdrSendFailures      0
GetDataBufFailures         0
GetBufHdrFailures          0
SendEackFailures           0
SendAckFailures            0
SendSynFailures            0
SendRstFailures            0
SendNullFailures           0
TimerNullFailures          0
FailedRetransmits          0
IncomingPktsDropped        0
UnknownRudpEvents          0
```

Field descriptions should be self-explanatory.

Related Commands

Command	Description
clear rudpv0 statistics	Resets the counters for the statistics generated by the **show rudpv0 failures** commandto 0.

Command	Description
show rudpv0 statistics	Displays RUDP information about number of packets sent, received, and so forth.

show rudpv0 statistics

To display SS7 Reliable User Datagram Protocol (RUDP) internal statistics, use the **show rudpv0 statistics** command in privileged EXEC command.

show rudpv0 statistics

Syntax Description

This command has no keywords or arguments.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.0(7)XR	This command was introduced.
12.1(1)T	This command was integrated into Cisco IOS Release 12.1(1)T.

Usage Guidelines

Because statistics counters are continually updated, the cumulative total may not be exactly equal to individual connection counters. After a connection is reset, previous statistics are lost, so the current connection statistics reflect only instances of the RUDP connection since the last reset.

Cumulative statistics reflect counts since the router was rebooted or since the **clear rudpv0 statistics** command was used.

Examples

The following is sample output from this command displaying RUDP statistics and states for two connections. The fields are self-explanatory.

```
Router# show rudpv0 statistics
*** RUDP Internal Stats ****
Connection ID: 811641AC,   Current State: OPEN
RcvdInSeq                  1
RcvdOutOfSeq               0
SoftResets                 0
SoftResetsRcvd             0
TotalPacketsSent           4828
TotalPacketsReceived       4826
TotalDataBytesSent         0
TotalDataBytesReceived     4
TotalDataPacketsSent       0
TotalDataPacketsReceived   1
TotalPacketsRetrans        0
TotalPacketsDiscarded      0
Connection ID: 81163FD4,   Current State: OPEN
RcvdInSeq                  2265
RcvdOutOfSeq               0
SoftResets                 0
SoftResetsRcvd             0
TotalPacketsSent           7863
TotalPacketsReceived       6755
TotalDataBytesSent         173690
TotalDataBytesReceived     56121
TotalDataPacketsSent       2695
TotalDataPacketsReceived   2265
```

```
TotalPacketsRetrans        0
TotalPacketsDiscarded      0
Cumulative RudpV0 Statistics
RcvdInSeq                  2266
RcvdOutOfSeq               0
SoftResets                 0
SoftResetsRcvd             0
TotalPacketsSent           12691
TotalPacketsReceived       11581
TotalDataBytesSent         173690
TotalDataBytesReceived     56125
TotalDataPacketsSent       2695
TotalDataPacketsReceived   2266
TotalPacketsRetrans        0
TotalPacketsDiscarded      0
```

Related Commands

Command	Description
clear rudpv0 statistics	Resets the counters for the statistics generated by the **show rudpv0 statistics** command to 0.
show rudpv0 failures	Displays RUDP information about failed connections and the reasons for them.

show rudpv1

To display Reliable User Datagram Protocol (RUDP) information, use the **show rudpv1** command in privileged EXEC mode.

show rudpv1 {**failures** | **parameters** | **statistics**}

Syntax Description

failures	RUDP failure statistics.
parameters	RUDP connection parameters.
statistics	RUDP internal statistics.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.1(1)T	This command was introduced on the Cisco AS5300.
12.2(2)T	This command was implemented on the Cisco 7200.
12.2(4)T	This command was implemented on the Cisco 2600 series, Cisco 3600 series, and Cisco MC3810.
12.2(2)XB1	This command was implemented on the Cisco AS5850.
12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T and implemented on the Cisco IAD2420 series.

Usage Guidelines

Because statistics counters are continually updated, the cumulative total may not be exactly equal to individual connection counters. After a connection is reset, previous statistics are lost, so the current connection statistics reflect only instances of the RUDP connection since the last reset.

Cumulative statistics reflect counts since the router was rebooted or since the **clear rudpv1 statistics** command was used.

Examples

The following is sample output from this command:

```
Router# show rudpv1 failures
**** RUDPV1 Failure Stats ****
CreateBufHdrsFailure       0
CreateConnRecsFailure      0
CreateEventQueueFailure    0
OsSpecificInitFailure      0
NotReadyFailures           0
OptionNotSupportedFailures 0
InvalidOptionFailures      0
OptionRequiredFailures     0
GetConnRecFailures         0
InvalidConnFailures        0
EventUnavailFailures       0
GetConnRecFailures         0
```

```
FindConnRecFailures         0
EmptyBufferSendFailures     0
BufferTooLargeFailures      0
ConnNotOpenFailures         0
SendWindowFullFailures      0
GetBufHdrSendFailures       0
SendInProgressFailures      0
GetDataBufFailures          0
GetBufHdrFailures           0
SendFailures                0
SendEackFailures            0
SendAckFailures             0
SendSynFailures             0
SendRstFailures             0
SendTcsFailures             0
SendNullFailures            0
TimerFailures               0
ApplQueueFailures           0
FailedRetransmits           0
IncomingPktsDropped         0
CksumErrors                 0
UnknownRudpv1Events         0
InvalidVersion              0
InvalidNegotiation          0
```

The following is sample output from the **show rudpv1 parameters** command:

```
Router# show rudpv1 parameters
*** RUDPV1 Connection Parameters ***
Next Connection Id:61F72B6C,  Remote conn id 126000
  Conn State              OPEN
  Conn Type               ACTIVE
  Accept Negot params?    Yes
  Receive Window          32
  Send Window             32
  Receive Seg Size        384
  Send Seg Size           384
                       Requested     Negotiated
  Max Auto Reset           5             5
  Max Cum Ack              3             3
  Max Retrans              2             2
  Max OutOfSeq             3             3
  Cum Ack Timeout        100           100
  Retrans Timeout        300           300
  Null Seg Timeout      1000          1000
  Trans State Timeout   2000          2000
  Cksum type             Hdr           Hdr
Next Connection Id:61F72DAC,  Remote conn id 126218
  Conn State              OPEN
  Conn Type               ACTIVE
  Accept Negot params?    Yes
  Receive Window          32
  Send Window             32
  Receive Seg Size        384
  Send Seg Size           384
                       Requested     Negotiated
  Max Auto Reset           5             5
  Max Cum Ack              3             3
  Max Retrans              2             2
  Max OutOfSeq             3             3
  Cum Ack Timeout        100           100
  Retrans Timeout        300           300
  Null Seg Timeout      1000          1000
```

```
  Trans State Timeout   2000          2000
  Cksum type             Hdr           Hdr
```

The following is sample output from **the show rudpv1 statistics** command:

```
Router# show rudpv1 statistics
*** RUDPV1 Internal Stats ****
Connection ID:61F72B6C,   Current State:OPEN
RcvdInSeq                  647
RcvdOutOfSeq               95
AutoResets                 0
AutoResetsRcvd             0
TotalPacketsSent           1011
TotalPacketsReceived       958
TotalDataBytesSent         17808
TotalDataBytesReceived     17808
TotalDataPacketsSent       742
TotalDataPacketsReceived   742
TotalPacketsRetrans        117
TotalPacketsDiscarded      38
Connection ID:61F72DAC,   Current State:OPEN
RcvdInSeq                  0
RcvdOutOfSeq               0
AutoResets                 0
AutoResetsRcvd             0
TotalPacketsSent           75
TotalPacketsReceived       75
TotalDataBytesSent         0
TotalDataBytesReceived     0
TotalDataPacketsSent       0
TotalDataPacketsReceived   0
TotalPacketsRetrans        0
TotalPacketsDiscarded      0
Cumulative RudpV1 Statistics
NumCurConnections          2
RcvdInSeq                  652
RcvdOutOfSeq               95
AutoResets                 0
AutoResetsRcvd             0
TotalPacketsSent           1102
TotalPacketsReceived       1047
TotalDataBytesSent         18048
TotalDataBytesReceived     18048
TotalDataPacketsSent       752
TotalDataPacketsReceived   752
TotalPacketsRetrans        122
TotalPacketsDiscarded      38
```

Related Commands

Command	Description
clear rudpv1 statistics	Clears the RUDP statistics counters.
debug rudpv1	Displays debugging information for RUDP.

show sccp

To display Skinny Client Control Protocol (SCCP) information such as administrative and operational status, use the **show sccp** command in user EXEC or privileged EXEC mode.

show sccp [**all** | **ccm group** [*number*] | **connections** [**details** | **internal** | **rsvp** | **summary**] | **server** | **statistics** | **call-identifications** | **call-references**]

Syntax Description

all	(Optional) Specifies all Skinny Client Control Protocol (SCCP) global information.
ccm	(Optional) Displays SCCP Cisco Unified Communications Manager (CUCM) group related information.
group	(Optional) Displays CUCM groups.
number	(Optional) CUCM group number that needs to be displayed.
connections	(Optional) Specifies information about the connections controlled by the SCCP transcoding and conferencing applications.
details	(Optional) Displays SCCP connections in detail.
internal	(Optional) Displays information about SCCP internal connections.
rsvp	(Optional) Displays Resource Reservation Protocol (RSVP) information about SCCP connections.
summary	(Optional) Displays information about SCCP connections.
server	(Optional) Displays SCCP server information.
statistics	(Optional) Specifies statistical information for SCCP transcoding and conferencing applications.
call-identifications	(Optional) Displays the following identification numbers that is associated with each leg of a call: • Session • Call Reference • Connection • Call • Bridge • Profile
call-references	(Optional) Displays codec, port, ID numbers for each leg of a call.

Command Modes

User EXEC
Privileged EXEC (#)

Command History

Release	Modification
12.1(5)YH	This command was introduced on the Cisco VG200.
12.2(6)T	This command was modified. The **rsvp**keyword was added.
12.2(13)T	This command was implemented on the Cisco 2600 series, Cisco 3620, Cisco 3640, Cisco 3660, and Cisco 3700 series.
12.3(8)T	This command was modified. The following keywords and arguments were added: **ccm**, **connections**, **details**, **group**, **internal,** *number,* **summary**.
12.4(11)XW1	This command was modified. The stype field was added to the show output to show whether a connections is encrypted.
12.4(15)XY	This command was modified. The **statistics** and **server**keywords were added.
12.4(22)T	This command was modified. Command output was updated to show IPv6 information and it was integrated into Cisco IOS Release 12.2(13)T.
15.1(4)M	This command was modified. The **call-identifications** and **call-references** keywords were added.

Usage Guidelines

The router on which you use the **show sccp** command must be equipped with one or more digital T1/E1 packet voice trunk network modules (NM-HDVs) or high-density voice (HDV) transcoding/conferencing DSP farms (NM-HDV-FARMs) to provide digital signal processor (DSP) resources.

Use the **show sccp ccm** group command to show detailed information about all groups assigned to the Cisco Unified CallManager. The optional group-number argument can be added to select details about a specific group.

Configure the **show sccp server statistics** command on the Cisco Unified Border Element, IP-to-IP Gateway, or Session Border Controller where no SCCP phone is registered, to show the statistical counts on the SCCP server. The counts display queuing errors and message drops on the transcoder alone when it is on the Cisco Unified Border Element, IP-to-IP Gateway, or Session Border Controller.

When the **show sccp server statistics** command is used on the Cisco Unified Manager Express (CME), it is recommended for use together with the clear sccp server statistics command.

Examples

In the following sample output, the gateway IP address can be an IPv4 or IPv6 address when it operates on an IPv4/IPv6 dual stack.

```
Router# show sccp
SCCP Admin State: UP
Gateway Local Interface: GigabitEthernet0/0
        IPv6 Address: 2001:DB8:C18:1::3
        IPv4 Address: 10.4.34.100
        Port Number: 2000
IP Precedence: 5
User Masked Codec list: None
Call Manager: 172.19.242.27, Port Number: 2000
```

```
                Priority: N/A, Version: 5.0.1, Identifier: 4
                Trustpoint: N/A
Call Manager: 2001:DB8:C18:1::100, Port Number: 2000
                Priority: N/A, Version: 7.0, Identifier: 1
                Trustpoint: N/A
```

The table below describes the significant fields shown in the display.

Table 128: show sccp Field Descriptions

Field	Description
SCCP Admin State	Current state of the SCCP session.
Gateway Local Interface	Local interface that SCCP applications use to register with Cisco Unified Communications Manager.
IP precedence	Sets the IP precedence value for SCCP.
User Masked Codec list	Codec to mask.
Call Manager	Cisco Unified CallManager server information.

The following is sample output from this command for IPv4 only. The field descriptions are self-explanatory.

```
Router# show sccp
SCCP Admin State: UP
Gateway IP Address: 10.10.10.11, Port Number: 0
Switchover Method: IMMEDIATE, Switchback Method: GUARD_TIMER
Switchback Guard Timer: 1200 sec, IP Precedence: 5
Max Supported MTP sessions: 100
Transcoding Oper State: ACTIVE - Cause Code: NONE
Active CallManager: 10.10.10.35, Port Number: 2000
TCP Link Status: CONNECTED
Conferencing Oper State: DOWN - Cause Code: DSPFARM_DOWN
Active CallManager: NONE
TCP Link Status: NOT_CONNECTED
CallManager: 10.10.10.37, Port Number: 2000
Priority: 3, Version: 3.1
CallManager: 10.10.10.35, Port Number: 2000
Priority: 2, Version: 3.0
```

The following sample shows statistical information for SCCP transcoding and conferencing applications.

```
Router# show sccp statistics
SCCP Transcoding Application Statistics:
TCP packets rx 548, tx 559
Unsupported pkts rx 3, Unrecognized pkts rx 0
Register tx 3, successful 3, rejected 0, failed 0
KeepAlive tx 543, successful 540, failed 2
OpenReceiveChannel rx 2, successful 2, failed 0
CloseReceiveChannel rx 0, successful 0, failed 0
StartMediaTransmission rx 2, successful 2, failed 0
StopMediaTransmission rx 0, successful 0, failed 0
MediaStreamingFailure rx 0
Switchover 1, Switchback 1
SCCP Conferencing Application Statistics:
TCP packets rx 0, tx 0
```

```
Unsupported pkts rx 0, Unrecognized pkts rx 0
Register tx 0, successful 0, rejected 0, failed 0
KeepAlive tx 0, successful 0, failed 0
OpenReceiveChannel rx 0, successful 0, failed 0
CloseReceiveChannel rx 0, successful 0, failed 0
StartMediaTransmission rx 0, successful 0, failed 0
StopMediaTransmission rx 0, successful 0, failed 0
MediaStreamingFailure rx 0
Switchover 0, Switchback 0
```

In the following example, the secure value of the stype field indicates that the conection is encrypted. The field descriptions are self-explanatory.

```
Router# show sccp connections
sess_id    conn_id    stype        mode codec   ripaddr       rport sport
16777222   16777409   secure-xcode sendrecv g729b   10.3.56.120   16772 19534
16777222   16777393   secure-xcode sendrecv g711u   10.3.56.50    17030 18464
Total number of active session(s) 1, and connection(s) 2
```

The following example shows the remote IP addresses of active RTP sessions, each of which shows either an IPv4 or an IPv6 address.

```
Router# show sccp connections
sess_id  conn_id  stype  mode    codec sport rport ripaddr
16777219 16777245 conf  sendrecv g711u 16516 27814 10.3.43.46
16777219 16777242 conf  sendrecv g711u 17712 18028 10.3.43.2
16777219 16777232 conf  sendrecv g711u 16890 19440 10.3.43.2
16777219 16777228 conf  sendrecv g711u 19452 17464 10.3.43.2
16777220 16777229 xcode sendrecv g711u 17464 19452 10.3.43.2
16777220 16777227 xcode sendrecv g729b 19466 19434 2001:0DB8:C18:1:212:79FF:FED7:B254
16777221 16777233 mtp   sendrecv g711u 19440 16890 10.3.43.2
16777221 16777231 mtp   sendrecv g711u 17698 17426 2001:0DB8:C18:1:212:79FF:FED7:B254
16777223 16777243 mtp   sendrecv g711u 18028 17712 10.3.43.2
16777223 16777241 mtp   sendrecv g711u 16588 19446 2001:0DB8:C18:1:212:79FF:FED7:B254
```

The following is sample output for the two Cisco CallManager Groups assigned to the Cisco Unified CallManager: group 5 named "boston office" and group 988 named "atlanta office".

```
Router# show sccp ccm group
CCM Group Identifier: 5
 Description: boston office
 Binded Interface: NONE, IP Address: NONE
 Registration Retries: 3, Registration Timeout: 10 sec
 Keepalive Retries: 3, Keepalive Timeout: 30 sec
 CCM Connect Retries: 3, CCM Connect Interval: 1200 sec
 Switchover Method: GRACEFUL, Switchback Method: GRACEFUL_GUARD
 Switchback Interval: 10 sec, Switchback Timeout: 7200 sec
 Signaling DSCP value: default, Audio DSCP value: default
CCM Group Identifier: 988
 Description: atlanta office
 Binded Interface: NONE, IP Address: NONE
 Associated CCM Id: 1, Priority in this CCM Group: 1
 Associated Profile: 6, Registration Name: MTP123456789988
 Associated Profile: 10, Registration Name: CFB123456789966
 Registration Retries: 3, Registration Timeout: 10 sec
 Keepalive Retries: 5, Keepalive Timeout: 30 sec
 CCM Connect Retries: 3, CCM Connect Interval: 10 sec
 Switchover Method: IMMEDIATE, Switchback Method: IMMEDIATE
 Switchback Interval: 15 sec, Switchback Timeout: 0 sec
 Signaling DSCP value: default, Audio DSCP value: default
```

The table below describes the significant fields shown in the display.

Table 129: show sccp ccm group Field Descriptions

Field	Description
CCM Group Identifier	Current state of the SCCP session.
Description	Local interface that SCCP applications use to register with Cisco Unified Communications Manager.
Binded Interface	Sets the IP precedence value for SCCP.
Registration Retries	Codec to mask.
Registration Timeout	Cisco Unified CallManager server information.
Keepalive Retries	Displays the number of keepalive retries from Skinny Client Control Protocol (SCCP) to Cisco Unified CallManager.
Keepalive Timeout	Displays the number of times that a DSP farm attempts to connect to a Cisco Unified CallManager.
CCM Connect Retries	Displays the amount of time, in seconds, that a given DSP farm profile waits before attempting to connect to a Cisco Unified CallManager when the current Cisco Unified CallManager fails to connect.
CCM Connect Interval	Method that the SCCP client uses when the communication link between the active Cisco Unified CallManager and the SCCP client fails.
Switchover Method	Method used when the secondary Cisco Unified CallManager initiates the switchback process with that higher order Cisco Unified CallManager.
Switchback Method	Method used when the secondary Cisco Unified CallManager initiates the switchback process with that higher order Cisco Unified CallManager.
Switchback Interval	Amount of time that the DSP farm waits before polling the primary Cisco Unified CallManager when the current Cisco Unified CallManager switchback connection fails.
Switchback Timeout	Amount of time, in seconds, that the secondary Cisco Unified CallManager waits before switching back to the primary Cisco Unified CallManager.
Associated CCM Id	Number assigned to the Cisco Unified CallManager.
Registration Name	User-specified device name in Cisco Unified CallManager.
Associated Profile	Number of the DSP farm profile associated with the Cisco Unified CallManager group.

The following sample output displays the summary information for all SCCP call references:

```
Router# show sccp call-reference
session_id: 16805277   session_type: vcf  , profile_id: 101,
    call-reference: 25666614  , Name: , Number: 3004
        Audio conn_id: 16777929  , str_passthr: 0
              rtp-call-id: 21        , bridge-id: 15        , msp-call-id: 12
              mode: sendrecv, sport: 25146, rport 16648, ripaddr: 10.22.82.205
```

```
            codec: g711u  , pkt-period: 20
    call-reference: 25666611  , Name: , Number: 6628
        Audio conn_id: 16777926  , str_passthr: 0
              rtp-call-id: 19        , bridge-id: 13        , msp-call-id: 12
              mode: sendrecv, sport: 28168, rport 2398 , ripaddr: 128.107.147.125
              codec: g711u  , pkt-period: 20
        Video conn_id: 16777927  , conn_id_tx: 16777928  , str_passthr: 0
              rtp-call-id: 20        , bridge-id: 14        , msp-call-id: 12
              mode: sendrecv, sport: 22604, rport 2400 , ripaddr: 128.107.147.125
              bit rate: 1100kbps, frame rate: 30fps , rtp pt_rx: 97, rtp pt_tx: 97
              codec: h264, Profile: 0x40, level: 2.2, max mbps: 81 (x500 MB/s), max fs: 7
(x256 MBs)
    call-reference: 25666608  , Name: , Number: 62783365
        Audio conn_id: 16777923  , str_passthr: 0
              rtp-call-id: 16        , bridge-id: 11        , msp-call-id: 12
              mode: sendrecv, sport: 21490, rport 20590, ripaddr: 10.22.83.142
              codec: g711u  , pkt-period: 20
        Video conn_id: 16777924  , conn_id_tx: 16777925  , str_passthr: 0
              rtp-call-id: 17        , bridge-id: 12        , msp-call-id: 12
              mode: sendrecv, sport: 23868, rport 29010, ripaddr: 10.22.83.142
              bit rate: 960kbps, frame rate: 30fps , rtp pt_rx: 97, rtp pt_tx: 97
              codec: h264, Profile: 0x40, level: 3.0, max mbps: 0 (x500 MB/s), max fs: 0
(x256 MBs)
    call-reference: 25666602  , Name: , Number: 62783363
        Audio conn_id: 16777916  , str_passthr: 0
              rtp-call-id: 11        , bridge-id: 7         , msp-call-id: 12
              mode: sendrecv, sport: 26940, rport 20672, ripaddr: 10.22.82.48
              codec: g711u  , pkt-period: 20
        Video conn_id: 16777917  , conn_id_tx: 16777919  , str_passthr: 0
              rtp-call-id: 13        , bridge-id: 8         , msp-call-id: 12
              mode: sendrecv, sport: 16462, rport 20680, ripaddr: 10.22.82.48
              bit rate: 960kbps, frame rate: 30fps , rtp pt_rx: 97, rtp pt_tx: 97
              codec: h264, Profile: 0x40, level: 2.0, max mbps: 72 (x500 MB/s), max fs: 5
(x256 MBs)
Total number of active session(s) 1
   Total of number of active session(s) 1
      with total of number of call-reference(s) 4
         with total of number of audio connection(s) 4
         with total of number of video connection(s) 3
```

The following sample output displays summary information for all SCCP call identifications:

```
Router# show sccp call-identifications
sess_id   callref   conn_id   conn_id_tx spid  rtp_callid msp_callid bridge_id  codec  stype
 prof_id
16805277  25666614  16777929  0          0     21         12         15         g711u  vcf
   101
16805277  25666611  16777926  0          0     19         12         13         g711u  vcf
   101
16805277  25666611  16777927  16777928   0     20         12         14         h264   vcf
   101
16805277  25666608  16777923  0          0     16         12         11         g711u  vcf
   101
16805277  25666608  16777924  16777925   0     17         12         12         h264   vcf
   101
16805277  25666602  16777916  0          0     11         12         7          g711u  vcf
   101
16805277  25666602  16777917  16777919   0     13         12         8          h264   vcf
   101
Total number of active session(s) 1
```

The following sample displays the output from show sccp:

```
Router# show sccp
SCCP Admin State: UP
Gateway Local Interface: GigabitEthernet0/1
        IPv4 Address: 172.19.156.7
        Port Number: 2000
IP Precedence: 5
User Masked Codec list: None
Call Manager: 1.4.211.39, Port Number: 2000
               Priority: N/A, Version: 7.0, Identifier: 1
               Trustpoint: N/A
Call Manager: 128.107.151.39, Port Number: 2000
               Priority: N/A, Version: 7.0, Identifier: 100
               Trustpoint: N/A
V_Conferencing Oper State: ACTIVE - Cause Code: NONE
Active Call Manager: 128.107.151.39, Port Number: 2000
TCP Link Status: CONNECTED, Profile Identifier: 101
Reported Max Streams: 4, Reported Max OOS Streams: 0
Layout: default 1x1
Supported Codec: g711ulaw, Maximum Packetization Period: 30
Supported Codec: g711alaw, Maximum Packetization Period: 30
Supported Codec: g729ar8, Maximum Packetization Period: 60
Supported Codec: g729abr8, Maximum Packetization Period: 60
Supported Codec: g729r8, Maximum Packetization Period: 60
Supported Codec: g729br8, Maximum Packetization Period: 60
Supported Codec: rfc2833 dtmf, Maximum Packetization Period: 30
Supported Codec: rfc2833 pass-thru, Maximum Packetization Period: 30
Supported Codec: inband-dtmf to rfc2833 conversion, Maximum Packetization Period: 30
Supported Codec: h264: QCIF, Frame Rate: 15fps, Bit Rate: 64-704 Kbps
Supported Codec: h264: QCIF, Frame Rate: 30fps, Bit Rate: 64-704 Kbps
Supported Codec: h264: CIF, Frame Rate: 15fps, Bit Rate: 64-704 Kbps
Supported Codec: h264: CIF, Frame Rate: 30fps, Bit Rate: 64-704 Kbps
Supported Codec: h264: 4CIF, Frame Rate: 30fps, Bit Rate: 1000-1000 Kbps
TLS : ENABLED
```

Related Commands

Command	Description
dsp service dspfarm	Configures DSP farm services for a specified voice card.
dspfarm (DSP farm)	Enables DSP-farm service.
dspfarm profile	Enters DSP farm profile configuration mode and defines a profile for DSP farm services.
sccp	Enables SCCP and its associated transcoding and conferencing applications.
show dspfarm	Displays summary information about DSP resources.

show sccp ccm group

To display the groups that are configured on a specific Cisco Unified CallManager, use the **show sccp ccm group**command in privileged EXEC mode.

show sccp ccm group [*group-number*]

Syntax Description

group-number	(Optional) Number that identifies the Cisco CallManager group. Range is 1 to 65535. There is no default value.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.3(8)T	This command was introduced.

Usage Guidelines

Use the **show sccp ccm group** command to show detailed information about all groups assigned to the Cisco Unified CallManager. The optional *group-number* argument can be added to select details about a specific group.

Examples

The following is sample output for the two Cisco CallManager Groups assigned to the Cisco Unified CallManager: group 5 named "boston office" and group 988 named "atlanta office".

```
Router# show sccp ccm group
CCM Group Identifier: 5
 Description: boston office
 Binded Interface: NONE, IP Address: NONE
 Registration Retries: 3, Registration Timeout: 10 sec
 Keepalive Retries: 3, Keepalive Timeout: 30 sec
 CCM Connect Retries: 3, CCM Connect Interval: 1200 sec
 Switchover Method: GRACEFUL, Switchback Method: GRACEFUL_GUARD
 Switchback Interval: 10 sec, Switchback Timeout: 7200 sec
 Signaling DSCP value: default, Audio DSCP value: default
CCM Group Identifier: 988
 Description: atlanta office
 Binded Interface: NONE, IP Address: NONE
 Associated CCM Id: 1, Priority in this CCM Group: 1
 Associated Profile: 6, Registration Name: MTP123456789988
 Associated Profile: 10, Registration Name: CFB123456789966
 Registration Retries: 3, Registration Timeout: 10 sec
 Keepalive Retries: 5, Keepalive Timeout: 30 sec
 CCM Connect Retries: 3, CCM Connect Interval: 10 sec
 Switchover Method: IMMEDIATE, Switchback Method: IMMEDIATE
 Switchback Interval: 15 sec, Switchback Timeout: 0 sec
 Signaling DSCP value: default, Audio DSCP value: default
```

The table below describes significant fields shown in this output.

Table 130: show sccp ccm group Field Descriptions

Field	Description
CCM Group Identifier	Displays the Cisco CallManager group number.
Description	Displays the optional description of the group assigned to the group number.
Binded Interface	Displays the IP address of the selected interface is used for all calls within a given profile.
Registration Retries	Number of times that SCCP tries to register with a Cisco Unified CallManger
Registration Timeout	Length of time, in seconds, between registration messages sent from SCCP to the Cisco Unified CallManager.
Keepalive Retries	Displays the number of keepalive retries from Skinny Client Control Protocol (SCCP) to Cisco Unified CallManager.
Keepalive Timeout	Displays the length of time, in seconds, between keepalive retries.
CCM Connect Retries	Displays the number of times that a DSP farm attempts to connect to a Cisco Unified CallManager.
CCM Connect Interval	Displays the amount of time, in seconds, that a given DSP farm profile waits before attempting to connect to a Cisco Unified CallManager when the current Cisco Unified CallManager fails to connect.
Switchover Method	Method that the SCCP client uses when the communication link between the active Cisco Unified CallManager and the SCCP client fails.
Switchback Method	Method used when the secondary Cisco Unified CallManager initiates the switchback process with that higher order Cisco Unified CallManager.
Switchback Interval	Amount of time that the DSP farm waits before polling the primary Cisco Unified CallManager when the current Cisco Unified CallManager switchback connection fails.
Switchback Timeout	Amount of time, in seconds, that the secondary Cisco Unified CallManager waits before switching back to the primary Cisco Unified CallManager.
Associated CCM Id	Number assigned to the Cisco Unified CallManager.
Registration Name	User-specified device name in Cisco Unified CallManager.
Associated Profile	Number of the DSP farm profile associated with the Cisco Unified CallManager group.

Related Commands

Command	Description
dspfarm profile	Enters DSP farm profile configuration mode and defines a profile for DSP farm services.
sccp ccm	Adds a Cisco Unified CallManager server to the list of available servers.

show sccp connections details

To display Skinny Client Control Protocol (SCCP) connection details such as call-leg details, use the **show sccp connections details** command in privileged EXEC mode.

show sccp connections details

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.3(8)T	This command was introduced.

Examples

The following is sample output from this command:

```
Router# show sccp connections details
bridge-info(bid, cid) - Normal bridge information(Bridge id, Calleg id)
mmbridge-info(bid, cid) - Mixed mode bridge information(Bridge id, Calleg id)
sess_id    conn_id    call-id    codec   pkt-period type      bridge-info(bid, cid)
mmbridge-info(bid, cid)
16800395   -          15         N/A     N/A        transmsp  All RTPSPI Callegs      N/A

16800395   18425889   14         g711u   20         rtpspi    (10,15)                 N/A

16800395   18425905   13         g711u   20         rtpspi    (9,15)                  N/A

Total number of active session(s) 1, connection(s) 2, and callegs 3
```

Related Commands

Command	Description
dspfarm profile	Enters DSP farm profile configuration mode and defines a profile for DSP farm services.
sccp ccm	Adds a Cisco CallManager server to the list of available servers and sets various parameters.
show sccp connections internal	Displays the internal SCCP details.
show sccp connections summary	Displays a summary of the number of SCCP sessions and connections.

show sccp connections internal

To display the internal Skinny Client Control Protocol (SCCP) details such as time-stamp values, use the **show sccp connections internal**command in privileged EXEC mode.

show sccp connections internal

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.3(8)T	This command was introduced.

Examples

The following is sample output from this command:

```
Router# show sccp connections internal
Total number of active session(s) 0, and connection(s) 0
```

Field descriptions should be self-explanatory.

Related Commands

Command	Description
dspfarm profile	Enters DSP farm profile configuration mode and defines a profile for DSP farm services.
sccp ccm	Adds a Cisco CallManager server to the list of available servers and sets various parameters.
show sccp connections details	Displays the SCCP connection details.
show sccp connections summary	Displays a summary of the number of SCCP sessions and connections.

show sccp connections rsvp

To display information about active Skinny Client Control Protocol (SCCP) connections that are using RSVP, use the **show sccp connections rsvp** command in privileged EXEC mode.

show sccp connections rsvp

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.4(6)T	This command was introduced.

Examples

The following is sample output from this command:

```
Router# show sccp connections rsvp
sess_id    conn_id    rsvp_id    dir  local ip       :port  remote ip      :port
16777578   16778093   -210       SEND 192.168.21.1   :18486 192.168.20.1   :16454
16777578   16778093   -211       RECV 192.168.21.1   :18486 192.168.20.1   :16454

 Total active sessions 1, connections 2, rsvp sessions 2
```

The table below describes the fields shown in the display.

Table 131: show sccp connections rsvp Field Descriptions

Field	Description
sess_id	Identification number of the SCCP session.
conn_id	Identification number of the SCCP connection.
rsvp_id	Identification number of the RSVP connection.
dir	Direction of the SCCP connection.
local ip	IP address of the local endpoint.
remote ip	IP address of the remote endpoint.
port	Port number of the local or remote endpoint.
Total active sessions	Total number of active SCCP sessions.
connections	Number of active connections that are a part of the SCCP sessions.
rsvp session	Number of active connections that use RSVP.

Related Commands

Command	Description
debug sccp all	Displays debugging information for SCCP.
dspfarm profile	Enters DSP farm profile configuration mode and defines a profile for DSP farm services.
rsvp	Enables RSVP support on a transcoding or MTP device.
sccp	Enables SCCP on the interface.
sccp local	Selects the local interface that SCCP applications use to register with Cisco Unified CallManager.
show sccp connections summary	Displays a summary of the number of SCCP sessions and connections.

show sccp connections summary

To display a summary of the number of sessions and connections based on the service type under the Skinny Client Control Protocol (SCCP) application, use the **show sccp connections summary** command in privileged EXEC mode.

show sccp connections summary

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.3(8)T	This command was introduced.

Examples

The following is sample output from this command:

```
Router# show sccp connections summary
SCCP Application Service(s) Statistics Summary:
Total Conferencing Sessions: 0, Connections: 0
Total Transcoding Sessions: 0, Connections: 0
Total MTP Sessions: 0, Connections: 0
Total SCCP Sessions: 0, Connections: 0
```

The table below describes significant fields shown in this output.

Table 132: show sccp connections summary Field Descriptions

Field	Description
Connections	Displays the total number of current connections associated with a given application.
Total Conferencing Sessions	Displays the number of current conferencing sessions.
Total MTP Sessions	Displays the number of current Media Termination Point (MTP) sessions.
Total SCCP Sessions	Displays the number of current SCCP sessions.
Total Transcoding Sessions	Displays the number of current transcoding sessions.

Related Commands

Command	Description
dspfarm profile	Enters DSP farm profile configuration mode and defines a profile for DSP farm services.
sccp ccm	Adds a Cisco CallManager server to the list of available servers and sets various parameters.

Command	Description
show sccp connections details	Displays the SCCP connection details.
show sccp connections internal	Displays the internal SCCP details.

show sccp server statistics

To display the statistical counts on the Skinny Client Control Protocol (SCCP) server, use the **show sccp server statistics** command in privileged EXEC mode.

show sccp server statistics

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.4(15)XY	This command was introduced.

Usage Guidelines

Configure the **show sccp server statistics** command on the Cisco Unified Border Element, IP-to-IP Gateway, or Session Border Controller where no SCCP phone is registered, to show the statistical counts on the SCCP server. The counts display queuing errors and message drops on the transcoder alone when it is on the Cisco Unified Border Element, IP-to-IP Gateway, or Session Border Controller.

When the **show sccp server statistics** command is used on the Cisco Unified Manager Express (CME), it is recommended for use together with the **clear sccp server statistics**command.

Examples

The following example shows the SCCP statistical counts on the server:

```
Router# show sccp server statistics
Failure type              Error count
------------------------  -----------
Send queue enqueue        2
Socket send               3
Msg discarded upon error  5
```

Field descriptions should be self-explanatory.

Related Commands

Command	Description
clear sccp server statistics	Clears the counts displayed the **under show sccp server statistics** command.

show sdspfarm

To display the status of the configured digital signal processor (DSP) farms and transcoding streams, use the **show sdspfarm**command in privileged EXEC mode.

show sdspfarm {**units** [**name** *unit-name* | **register** | **summary** | **tag** *number* | **unregister**] | **sessions** [**active** | **callID** *number* | **states** | **statistics** | **streamID** *number* | **summary**] | **message statistics**} [**video**]

Syntax Description

units	Displays the configured and registered DSP farms.
name *unit-name*	(Optional) Displays the name of the unit.
register	(Optional) Displays information about the registered units.
summary	(Optional) Displays summary information about the units.
tag *number*	(Optional) Displays the tag number of the unit.
unregister	(Optional) Displays information about the unregistered units.
sessions	Displays the transcoding streams.
active	(Optional) Displays all active sessions.
callID	(Optional) Displays activities for a specific caller ID.
number	(Optional) The caller ID number displayed by the **show voip rtp connection** command.
states	(Optional) Displays the current state of the transcoding stream.
statistics	(Optional) Displays session statistics.
streamID *number*	(Optional) Displays the transcoding stream sequence number.
summary	(Optional) Displays summary information.
message	Displays message information.
statistics	Displays statistics information about the messages.
video	(Optional) Displays information on video streams.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.3(11)T	This command was introduced.
12.4(22)T	The following combinations of keywords and arguments were added: **name**, *unit-name*, **register**, **summary**, **tag** *number*, **unregister**, **states**, **streamID** *number*, **message statistics**.

Release	Modification
15.1(4)M	The **video** keyword was added.

Examples

The following example displays the configured and registered DSP farms:

```
Router# show sdspfarm units
mtp-1 Device:MTP123456782012 TCP socket:[-1]  UNREGISTERED
actual_stream:0 max_stream 0 IP:0.0.0.0  0  Unknown 0 keepalive 0
mtp-2 Device:MTP000a8aeaca80 TCP socket:[5]  REGISTERED
actual_stream:40 max_stream 40 IP:10.5.49.160  11001  MTP YOKO keepalive 12074
Supported codec:G711Ulaw
                G711Alaw
                G729
                G729a
                G729b
                G729ab
 max-mtps:2, max-streams:240, alloc-streams:40, act-streams:0
```

The following is sample output from the **show sdspfarm sessions active**command:

```
Router# show sdspfarm sessions active
Stream-ID:3 mtp:2 192.0.2.0 20174  Local:2000 START
 usage:MoH  (DN=3  , CH=1) FE=TRUE
 codec:G729  duration:20 vad:0 peer Stream-ID:4
Stream-ID:4 mtp:2 192.0.2.0 17072  Local:2000 START
 usage:MoH  (DN=3  , CH=1) FE=FALSE
 codec:G711Ulaw64k  duration:20 vad:0 peer Stream-ID:3
```

The following is sample output from the **show sdspfarm sessions callID**command:

```
Router# show sdspfarm sessions callID 51
Stream-ID:6, srcCall-ID:51, codec:G729AnnexA , dur:20ms, vad:0, dstCall-ID:52, confID:5,
mtp:2^
Peer Stream-ID:5, srcCall-ID:52, codec:G711Ulaw64k , dur:20ms, vad:0, dstCall-ID:51, confID:5,
 mtp:2^
Router-2015# show sdspfarm sessions callid 52
Stream-ID:5, srcCall-ID:52, codec:G711Ulaw64k , dur:20ms, vad:0, dstCall-ID:51, confID:5,
mtp:2
Peer Stream-ID:6, srcCall-ID:51, codec:G729AnnexA , dur:20ms, vad:0, dstCall-ID:52, confID:5,
 mtp:2
```

The following is sample output from the **show sdspfarm sessions statistics**command:

```
Router# show sdspfarm sessions statistics
Stream-ID:1 mtp:2 0.0.0.0  0  Local:0IDLE
 codec:G711Ulaw64k  duration:20 vad:0 peer Stream-ID:0
 recv-pak:0 xmit-pak:0 out-pak:1014 in-pak:0 discard:0
Stream-ID:2 mtp:2 0.0.0.0  0  Local:0IDLE
 codec:G711Ulaw64k  duration:20 vad:0 peer Stream-ID:0
 recv-pak:0 xmit-pak:0 out-pak:0 in-pak:0 discard:0
Stream-ID:3 mtp:2 10.5.49.160  20174  Local:2000START  MoH  (DN=3  , CH=1) FE=TRUE
 codec:G729  duration:20 vad:0 peer Stream-ID:4
 recv-pak:0 xmit-pak:0 out-pak:4780 in-pak:0 discard:0
Stream-ID:4 mtp:2 10.5.49.160  17072  Local:2000START  MoH  (DN=3  , CH=1) FE=FALSE
 codec:G711Ulaw64k  duration:20 vad:0 peer Stream-ID:3
 recv-pak:0 xmit-pak:0 out-pak:0 in-pak:0 discard:0
Stream-ID:5 mtp:2 0.0.0.0  0  Local:0IDLE
 codec:G711Ulaw64k  duration:20 vad:0 peer Stream-ID:0
```

```
 recv-pak:0 xmit-pak:0 out-pak:0 in-pak:0 discard:0
Stream-ID:6 mtp:2 0.0.0.0  0  Local:0IDLE
 codec:G711Ulaw64k  duration:20 vad:0 peer Stream-ID:0
 recv-pak:0 xmit-pak:0 out-pak:0 in-pak:0 discard:0
Stream-ID:7 mtp:2 0.0.0.0  0  Local:0IDLE
 codec:G711Ulaw64k  duration:20 vad:0 peer Stream-ID:0
 recv-pak:0 xmit-pak:0 out-pak:0 in-pak:0 discard:0
Stream-ID:8 mtp:2 0.0.0.0  0  Local:0IDLE
 codec:G711Ulaw64k  duration:20 vad:0 peer Stream-ID:0
 recv-pak:0 xmit-pak:0 out-pak:0 in-pak:0 discard:0
Stream-ID:9 mtp:2 0.0.0.0  0  Local:0IDLE
 codec:G711Ulaw64k  duration:20 vad:0 peer Stream-ID:0
 recv-pak:0 xmit-pak:0 out-pak:0 in-pak:0 discard:0
Stream-ID:10 mtp:2 0.0.0.0  0  Local:0IDLE
 codec:G711Ulaw64k  duration:20 vad:0 peer Stream-ID:0
 recv-pak:0 xmit-pak:0 out-pak:0 in-pak:0 discard:0
Stream-ID:11 mtp:2 0.0.0.0  0  Local:0IDLE
 codec:G711Ulaw64k  duration:20 vad:0 peer Stream-ID:0
 recv-pak:0 xmit-pak:0 out-pak:0 in-pak:0 discard:0
Stream-ID:12 mtp:2 0.0.0.0  0  Local:0IDLE
 codec:G711Ulaw64k  duration:20 vad:0 peer Stream-ID:0
 recv-pak:0 xmit-pak:0 out-pak:0 in-pak:0 discard:0
Stream-ID:13 mtp:2 0.0.0.0  0  Local:0IDLE
 codec:G711Ulaw64k  duration:20 vad:0 peer Stream-ID:0
 recv-pak:0 xmit-pak:0 out-pak:0 in-pak:0 discard:0
Stream-ID:14 mtp:2 0.0.0.0  0  Local:0IDLE
 codec:G711Ulaw64k  duration:20 vad:0 peer Stream-ID:0
 recv-pak:0 xmit-pak:0 out-pak:0 in-pak:0 discard:0
Stream-ID:15 mtp:2 0.0.0.0  0  Local:0IDLE
 codec:G711Ulaw64k  duration:20 vad:0 peer Stream-ID:0
 recv-pak:0 xmit-pak:0 out-pak:0 in-pak:0 discard:0
Stream-ID:16 mtp:2 0.0.0.0  0  Local:0IDLE
 codec:G711Ulaw64k  duration:20 vad:0 peer Stream-ID:0
 recv-pak:0 xmit-pak:0 out-pak:0 in-pak:0 discard:0
Stream-ID:17 mtp:2 0.0.0.0  0  Local:0IDLE
 codec:G711Ulaw64k  duration:20 vad:0 peer Stream-ID:0
 recv-pak:0 xmit-pak:0 out-pak:0 in-pak:0 discard:0
Stream-ID:18 mtp:2 0.0.0.0  0  Local:0IDLE
 codec:G711Ulaw64k  duration:20 vad:0 peer Stream-ID:0
 recv-pak:0 xmit-pak:0 out-pak:0 in-pak:0 discard:0
Stream-ID:19 mtp:2 0.0.0.0  0  Local:0IDLE
 codec:G711Ulaw64k  duration:20 vad:0 peer Stream-ID:0
 recv-pak:0 xmit-pak:0 out-pak:0 in-pak:0 discard:0
Stream-ID:20 mtp:2 0.0.0.0  0  Local:0IDLE
 codec:G711Ulaw64k  duration:20 vad:0 peer Stream-ID:0
 recv-pak:0 xmit-pak:0 out-pak:0 in-pak:0 discard:0
Stream-ID:21 mtp:2 0.0.0.0  0  Local:0IDLE
 codec:G711Ulaw64k  duration:20 vad:0 peer Stream-ID:0
 recv-pak:0 xmit-pak:0 out-pak:0 in-pak:0 discard:0
Stream-ID:22 mtp:2 0.0.0.0  0  Local:0IDLE
 codec:G711Ulaw64k  duration:20 vad:0 peer Stream-ID:0
 recv-pak:0 xmit-pak:0 out-pak:0 in-pak:0 discard:0
Stream-ID:23 mtp:2 0.0.0.0  0  Local:0IDLE
 codec:G711Ulaw64k  duration:20 vad:0 peer Stream-ID:0
 recv-pak:0 xmit-pak:0 out-pak:0 in-pak:0 discard:0
Stream-ID:24 mtp:2 0.0.0.0  0  Local:0IDLE
 codec:G711Ulaw64k  duration:20 vad:0 peer Stream-ID:0
 recv-pak:0 xmit-pak:0 out-pak:0 in-pak:0 discard:0
Stream-ID:25 mtp:2 0.0.0.0  0  Local:0IDLE
 codec:G711Ulaw64k  duration:20 vad:0 peer Stream-ID:0
 recv-pak:0 xmit-pak:0 out-pak:0 in-pak:0 discard:0
Stream-ID:26 mtp:2 0.0.0.0  0  Local:0IDLE
 codec:G711Ulaw64k  duration:20 vad:0 peer Stream-ID:0
 recv-pak:0 xmit-pak:0 out-pak:0 in-pak:0 discard:0
```

```
Stream-ID:27 mtp:2 0.0.0.0  0  Local:0IDLE
 codec:G711Ulaw64k  duration:20 vad:0 peer Stream-ID:0
 recv-pak:0 xmit-pak:0 out-pak:0 in-pak:0 discard:0
Stream-ID:28 mtp:2 0.0.0.0  0  Local:0IDLE
 codec:G711Ulaw64k  duration:20 vad:0 peer Stream-ID:0
 recv-pak:0 xmit-pak:0 out-pak:0 in-pak:0 discard:0
Stream-ID:29 mtp:2 0.0.0.0  0  Local:0IDLE
 codec:G711Ulaw64k  duration:20 vad:0 peer Stream-ID:0
 recv-pak:0 xmit-pak:0 out-pak:0 in-pak:0 discard:0
Stream-ID:30 mtp:2 0.0.0.0  0  Local:0IDLE
 codec:G711Ulaw64k  duration:20 vad:0 peer Stream-ID:0
 recv-pak:0 xmit-pak:0 out-pak:0 in-pak:0 discard:0
Stream-ID:31 mtp:2 0.0.0.0  0  Local:0IDLE
 codec:G711Ulaw64k  duration:20 vad:0 peer Stream-ID:0
 recv-pak:0 xmit-pak:0 out-pak:0 in-pak:0 discard:0
Stream-ID:32 mtp:2 0.0.0.0  0  Local:0IDLE
 codec:G711Ulaw64k  duration:20 vad:0 peer Stream-ID:0
 recv-pak:0 xmit-pak:0 out-pak:0 in-pak:0 discard:0
Stream-ID:33 mtp:2 0.0.0.0  0  Local:0IDLE
 codec:G711Ulaw64k  duration:20 vad:0 peer Stream-ID:0
 recv-pak:0 xmit-pak:0 out-pak:0 in-pak:0 discard:0
Stream-ID:34 mtp:2 0.0.0.0  0  Local:0IDLE
 codec:G711Ulaw64k  duration:20 vad:0 peer Stream-ID:0
 recv-pak:0 xmit-pak:0 out-pak:0 in-pak:0 discard:0
Stream-ID:35 mtp:2 0.0.0.0  0  Local:0IDLE
 codec:G711Ulaw64k  duration:20 vad:0 peer Stream-ID:0
 recv-pak:0 xmit-pak:0 out-pak:0 in-pak:0 discard:0
Stream-ID:36 mtp:2 0.0.0.0  0  Local:0IDLE
 codec:G711Ulaw64k  duration:20 vad:0 peer Stream-ID:0
 recv-pak:0 xmit-pak:0 out-pak:0 in-pak:0 discard:0
Stream-ID:37 mtp:2 0.0.0.0  0  Local:0IDLE
 codec:G711Ulaw64k  duration:20 vad:0 peer Stream-ID:0
 recv-pak:0 xmit-pak:0 out-pak:0 in-pak:0 discard:0
Stream-ID:38 mtp:2 0.0.0.0  0  Local:0IDLE
 codec:G711Ulaw64k  duration:20 vad:0 peer Stream-ID:0
 recv-pak:0 xmit-pak:0 out-pak:0 in-pak:0 discard:0
Stream-ID:39 mtp:2 0.0.0.0  0  Local:0IDLE
 codec:G711Ulaw64k  duration:20 vad:0 peer Stream-ID:0
 recv-pak:0 xmit-pak:0 out-pak:0 in-pak:0 discard:0
Stream-ID:40 mtp:2 0.0.0.0  0  Local:0IDLE
 codec:G711Ulaw64k  duration:20 vad:0 peer Stream-ID:0
 recv-pak:0 xmit-pak:0 out-pak:0 in-pak:0 discard:0
```

The following is sample output from the **show sdspfarm sessions summary**command:

```
Router# show sdspfarm sessions summary
max-mtps:2, max-streams:240, alloc-streams:40, act-streams:2
  ID   MTP  State      CallID confID Usage                          Codec/Duration
==== ===== ====== ========== ====== ============================== ==============
1    2     IDLE   -1         0                                     G711Ulaw64k /20ms
2    2     IDLE   -1         0                                     G711Ulaw64k /20ms
3    2     START  -1         3      MoH  (DN=3  , CH=1) FE=TRUE  G729 /20ms
4    2     START  -1         3      MoH  (DN=3  , CH=1) FE=FALSE G711Ulaw64k /20ms
5    2     IDLE   -1         0                                     G711Ulaw64k /20ms
6    2     IDLE   -1         0                                     G711Ulaw64k /20ms
7    2     IDLE   -1         0                                     G711Ulaw64k /20ms
8    2     IDLE   -1         0                                     G711Ulaw64k /20ms
9    2     IDLE   -1         0                                     G711Ulaw64k /20ms
10   2     IDLE   -1         0                                     G711Ulaw64k /20ms
11   2     IDLE   -1         0                                     G711Ulaw64k /20ms
12   2     IDLE   -1         0                                     G711Ulaw64k /20ms
13   2     IDLE   -1         0                                     G711Ulaw64k /20ms
14   2     IDLE   -1         0                                     G711Ulaw64k /20ms
15   2     IDLE   -1         0                                     G711Ulaw64k /20ms
```

```
16   2     IDLE   -1          0                                    G711Ulaw64k /20ms
17   2     IDLE   -1          0                                    G711Ulaw64k /20ms
18   2     IDLE   -1          0                                    G711Ulaw64k /20ms
19   2     IDLE   -1          0                                    G711Ulaw64k /20ms
20   2     IDLE   -1          0                                    G711Ulaw64k /20ms
21   2     IDLE   -1          0                                    G711Ulaw64k /20ms
22   2     IDLE   -1          0                                    G711Ulaw64k /20ms
23   2     IDLE   -1          0                                    G711Ulaw64k /20ms
24   2     IDLE   -1          0                                    G711Ulaw64k /20ms
25   2     IDLE   -1          0                                    G711Ulaw64k /20ms
26   2     IDLE   -1          0                                    G711Ulaw64k /20ms
27   2     IDLE   -1          0                                    G711Ulaw64k /20ms
28   2     IDLE   -1          0                                    G711Ulaw64k /20ms
29   2     IDLE   -1          0                                    G711Ulaw64k /20ms
30   2     IDLE   -1          0                                    G711Ulaw64k /20ms
31   2     IDLE   -1          0                                    G711Ulaw64k /20ms
32   2     IDLE   -1          0                                    G711Ulaw64k /20ms
33   2     IDLE   -1          0                                    G711Ulaw64k /20ms
34   2     IDLE   -1          0                                    G711Ulaw64k /20ms
35   2     IDLE   -1          0                                    G711Ulaw64k /20ms
36   2     IDLE   -1          0                                    G711Ulaw64k /20ms
37   2     IDLE   -1          0                                    G711Ulaw64k /20ms
38   2     IDLE   -1          0                                    G711Ulaw64k /20ms
39   2     IDLE   -1          0                                    G711Ulaw64k /20ms
40   2     IDLE   -1          0                                    G711Ulaw64k /20ms
```

The table below describes the fields shown in the **show sdspfarm** command display.

Table 133: show sdspfarm Field Descriptions

Field	Description
act-streams	Active streams that are involved in calls.
alloc-streams	Number of transcoding streams that are actually allocated to all DSP farms that are registered to Cisco CME.
callID	Caller ID that the active stream is in.
Codec	Codec in use.
confID	ConfID that is used to communicate with DSP farms.
discard	Number of packets that are discarded.
dstCall-ID	Caller ID of the destination IP call leg.
Duration or dur	Packet rates, in milliseconds.
ID	Transcoding stream sequence number in Cisco CME.
in-pak	Number of incoming packets from the source call leg.
Local	Local port for voice packets.
max-mtps	Maximum number of Message Transfer Parts (MTPs) that are allowed to register in Cisco CME.
max-streams	Maximum number of transcoding streams that are allowed in Cisco CME.

Field	Description
mtp or MTP	MTP sequence number where the transcoding stream is located.
out-pak	Number of outgoing packets sending to source call leg.
peer Stream-ID	Stream sequence number of the other stream paired in the same transcoding session. (Two transcoding streams make up a transcoding session).
recv-pak	Number of voice packets received from the DSP farm.
srcCall-ID	Source caller ID of the source IP call leg.
State	Current state of the transcoding stream; could be IDLE, SEIZE, START, STOP, or END.
Stream-ID	Transcoding stream sequence number in Cisco CME.
TCP socket	Socket number for DSP farm (similar to TCP socket for **show ephone** output).
usage	Current usage of the stream; for example, Ip-Ip (IP to IP transcoding), Moh (for MOH transcoding) and Conf (conference).
vad	Voice-activity detection (VAD) flag for the transcoding stream. It should always be 0 (False).
xmit-pak	Number of packets that are sent to the DSP farm.

Related Commands

Command	Description
sdspfarm tag	Permits a DSP farm to be to registered to Cisco CME and be associated with an SCCP client interface's MAC address.
sdspfarm transcode sessions	Specifies the maximum number of transcoding sessions allowed per Cisco CME router.
sdspfarm units	Specifies the maximum number of DSP farms that are allowed to be registered to Cisco CME.

show settlement

To display the configuration for all settlement servers and see specific provider and transactions, use the **show settlement** command in privileged EXEC mode.

show settlement [**provider-number** [**transactions**]]

Syntax Description

provider -number	(Optional) Displays the attributes of a specific provider.
transactions	(Optional) Displays the transaction status of a specific provider.

Command Default

Information about all servers is displayed.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.0(4)XH1	This command was introduced on the Cisco 2600 series, Cisco 3600 series, and Cisco AS5300.
12.1(1)T	This command was integrated into Cisco IOS Release 12.1(1)T.

Examples

The following is sample output from this command displaying information about all settlement servers that are configured:

```
Router# show settlement
Settlement Provider 0
Type = osp
Address url = https://1.14.115.100:6556/
Encryption = all                (default)
Max Concurrent Connections = 20 (default)
Connection Timeout = 3600 (s)   (default)
Response Timeout = 1 (s)        (default)
Retry Delay = 2 (s)             (default)
Retry Limit = 1                 (default)
Session Timeout = 86400 (s)     (default)
Customer Id = 1000
Device Id = 1000
Roaming = Disabled              (default)
Signed Token = on
Number of Connections = 0
Number of Transactions = 7
```

The following is sample output from this command displaying transaction and state information about a specific settlement server:

```
Router# show settlement 0 transactions
Transaction ID=8796304133625270342
        state=OSPC_GET_DEST_SUCCESS, index=0
        callingNumber=5710868, calledNumber=15125551212
```

The table below describes significant fields shown in this output. Provider attributes that are not configured are not shown.

Table 134: show settlement Field Descriptions

Field	Description
type	Settlement provider type.
address url	URL address of the provider.
encryption	SSL encryption method.
max-connections	Maximum number of concurrent connections to provider.
connection-timeout	Connection timeout with provider (in seconds).
response-timeout	Response timeout with provider (in seconds).
retry-delay	Delay time between retries (in seconds).
retry-limit	Number of retries.
session-timeout	SSL session timeout (in seconds).
customer-id	Customer ID, assigned by provider.
device-id	Device ID, assigned by provider.
roaming	Roaming enabled.
signed-token	Indicates if the settlement token is signed by the server.

Related Commands

Command	Description
connection -timeout	Configures the time that a connection is maintained after a communication exchange is completed.
customer -id	Identifies a carrier or ISP with a settlement provider.
device -id	Specifies a gateway associated with a settlement provider.
encryption	Sets the encryption method to be negotiated with the provider.
max -connection	Sets the maximum number of simultaneous connections to be used for communication with a settlement provider.
response -timeout	Configures the maximum time to wait for a response from a server.
retry -delay	Sets the time between attempts to connect with the settlement provider.
session -timeout	Sets the interval for closing the connection when there is no input or output traffic.
settlement	Enters settlement configuration mode and specifies the attributes specific to a settlement provider.
type	Configures an SAA-RTR operation type.

show sgcp connection

To display all active Simple Gateway Control Protocol (SGCP) connections on a router, use the **show sgcp connection**command in EXEC mode.

show sgcp connection [**interface** *number*]

Syntax Description

interface	(Optional) Displays output for a particular DS1 interface.
number	(Optional) Interface (controller) number.

Command Default

All active SGCP connections on the host are displayed.

Command Modes

EXEC (>)

Command History

Release	Modification
12.0(5)T	This command was introduced in a private release on the Cisco AS5300 only and was not generally available.
12.0(7)XK	This command was implemented on the Cisco MC3810 and Cisco 3600 series (except for the Cisco 3620) in a private release that was not generally available.

Examples

The following is sample output from thiscommand displaying active connections on a router:

```
Router# show sgcp connection
Endpoint        Call_ID(C) Conn_ID(I) (P)ort (M)ode (S)tate (E)vent[SIFL] (R)esult[EA]
1. ds1-0/1@r3810-5      C=1,1,2  I=0x1  P=16492,16476  M=3  S=4  E=3,0,0,3  R=0, 0
```

The following is sample output from thiscommand displaying the state of SGCP on a router:

```
Router# show sgcp connection
SGCP Admin State DOWN, Oper State DOWN
SGCP call-agent:
209.165.200.225
 , SGCP graceful-shutdown enabled? FALSE
SGCP request timeout 40, SGCP request retries 10
```

The table below describes significant fields shown in this output.

Table 135: show sgcp connection Field Descriptions

Field	Description
SGCP Admin State	Administrative and operational state of the SGCP daemon.
SGCP call-agent	Address of the call agent specified with the **sgcp** command.
SGCP graceful-shutdown enabled	The state of the **sgcp graceful-shutdown** command.

Field	Description
SGCP request timeout	The setting for the **sgcp request timeout** command.
SGCP request retries	The setting for the **sgcp request retries** command.

Related Commands

Command	Description
show sgcp endpoint	Displays SGCP endpoint information.
show sgcp statistics	Displays global statistics for the SGCP packet count, success, and failure counts.

show sgcp endpoint

To display Simple Gateway Control Protocol (SGCP) endpoints that are eligible for SGCP management, use the **show sgcp endpoint** command in EXEC mode.

show sgcp endpoint [**interface** *ds1* [*ds0*]]

Syntax Description

interface *ds1*	(Optional) DS1 interface for which to display SGCP endpoint information. Range is from 1 to 1000.
ds0	(Optional) DS0 interface for which to display SGCP endpoint information. Range is from 0 to 30.

Command Modes

EXEC (#)

Command History

Release	Modification
12.0(5)T	This command was introduced in a private release on the Cisco AS5300 only and was not generally available.
12.0(7)XK	This command was implemented on the Cisco MC3810 and Cisco 3600 series (except for the Cisco 3620) in a private release that was not generally available.

Usage Guidelines

Use this command to display SGCP endpoint information for the whole router or for a specific DS1 interface and, optionally, a specific DS0. If you enter a nonexistent combination of a DS1 and DS0, the following error message appears: "No matching connection found."

Examples

The following is sample output from this command displaying SGCP endpoint information being set for a matching connection between DS1 interface 1 and DS0 interface 10:

```
Router# show sgcp endpoint interface 1 10
```

Related Commands

Command	Description
show sgcp connection	Displays all the active connections on the host router.
show sgcp statistics	Displays global statistics for the SGCP packet count, success, and failure counts.

show sgcp statistics

To display global statistics for the Simple Gateway Control Protocol (SGCP) packet count, success and failure counts, and other information, use the **show sgcp statistics** command in EXEC mode.

show sgcp statistics

Syntax Description

This command has no arguments or keywords.

Command Modes

EXEC (#)

Command History

Release	Modification
12.0(7)XK	This command was introduced on the Cisco MC3810 and Cisco 3600 series (except for the Cisco 3620) in a private release that was not generally available.
12.0(5)T	This command was implemented on the Cisco AS5300 only in a private release that was not generally available.

Usage Guidelines

You can filter the displayed output, as shown in the examples.

Examples

The following is sample output from this command displaying SGCP packet statistics:

```
Router# show sgcp statistics
UDP pkts rx 5, tx 13
Unrecognized rx pkts 0, SGCP message parsing errors 0
Duplicate SGCP ack tx 0
Failed to send SGCP messages 0
CreateConn rx 1, successful 1, failed 0
DeleteConn rx 0, successful 0, failed 0
ModifyConn rx 0, successful 0, failed 0
DeleteConn tx 0, successful 0, failed 0
NotifyRequest rx 3, successful 3, failed 0
Notify tx 3, successful 3, failed 0
ACK tx 4, NACK tx 0
ACK rx 1, NACK rx 0
IP address based Call Agents statistics:
IP address 1.4.63.100, Total msg rx 5,
                   successful 5, failed 2
```

The following is sample output from this command showing how to filter output for specific information:

```
Router# show sgcp statistics | begin Failed
Failed to send SGCP messages 0
CreateConn rx 0, successful 0, failed 0
DeleteConn rx 0, successful 0, failed 0
ModifyConn rx 0, successful 0, failed 0
DeleteConn tx 0, successful 0, failed 0
NotifyRequest rx 0, successful 0, failed 0
Notify tx 0, successful 0, failed 0
ACK tx 0, NACK tx 0
ACK rx 0, NACK rx 0
```

```
Router# show sgcp statistics | exclude ACK
UDP pkts rx 0, tx 0
Unrecognized rx pkts 0, SGCP message parsing errors 0
Duplicate SGCP ack tx 0
Failed to send SGCP messages 0
CreateConn rx 0, successful 0, failed 0
DeleteConn rx 0, successful 0, failed 0
ModifyConn rx 0, successful 0, failed 0
DeleteConn tx 0, successful 0, failed 0
NotifyRequest rx 0, successful 0, failed 0
Notify tx 0, successful 0, failed 0
Router# show sgcp statistics | include ACK
ACK tx 0, NACK tx 0
ACK rx 0, NACK rx 0
```

Related Commands

Command	Description
show sgcp connection	Displays all the active connections on the host Cisco AS5300 universal access server.
show sgcp endpoint	Displays SGCP endpoint information.

show shared-line

To display information about the Session Initiation Protocol (SIP) shared lines, use the **show shared-line** command in user EXEC or privileged EXEC mode.

show shared-line {**call** | **details** | **subscription** | **summary**}

Syntax Description

call	Displays information about all active calls on shared lines.
details	Displays detailed information about each shared line.
subscription	Displays information for specific subscriptions to shared lines.
summary	Displays summary information about active subscriptions to shared lines.

Command Modes

User EXEC (>)
Privileged EXEC (#)

Command History

Release	Modification
12.4(24)T	This command was introduced.

Examples

The following is sample output from the **show shared-line call** command:

```
Router# show shared-line call
Shared-Line active call info:
Shared-Line: '20141',  active calls: 3
Local User       Local Address               Remote User       Remote Address   CallID
==========       =====================       ===========       ==================== ====
20141            20141@10.6.0.2               20143             20143@10.10.0.1  3168

20141            20141@10.6.0.1               Barge             20143@10.10.0.1  3209

20141            20141@10.6.0.2               20141             20141@10.10.0.1  3210
```

The following is sample output from the **show shared-line details** command:

```
Router# show shared-line details
Shared-Line info details:

Shared-Line: '20141',  subscribed users: 2,  max calls limit: 10
Index        Users                 sub_id         peer_tag        Status
=====        =====                 ======         ========        ======
  1          20141@10.6.0.1             5            40001          ACTIVE
  2          20141@10.6.0.2             6            40002          ACTIVE
Free call queue size: 7,   Active call queue size: 3

Message queue size: 20,   Event queue size: 64
```

The following is sample output from the **show shared-line subscription** command:

```
Router# show shared-line subscription
Shared-Line Subscription Info:

Subscriptions to: '20141',   total subscriptions: 2
SubID        Subscriber                  Expires         Sub-Status
=====        ==========                  =======         ==========
  5          20141@10.6.0.1                 3600          NOTIFY_ACKED
  6          20141@10.6.0.2                 3600          NOTIFY_ACKED
```

The following is sample output from the **show shared-line summary** command:

```
Router# show shared-line summary
Shared-Line info summary:
Shared-Line: '20141',  subscribed users: 2,  max calls limit: 10
```

The table below describes the significant fields shown in the displays.

Table 136: show shared-line Field Descriptions

Field	Description
Expires	Number of seconds until the subscription expires.
Local Address	IP address of the local phone involved in the shared line call.
Local User	Extension number of the shared line.
Remote Address	IP address of the remote phone involved in the shared line call.
Remote User	Extension of the remote phone involved in the shared line call.
SubID	Subscription ID.
Subscriber	Extension number of the shared line and the IP address of the phone subscriber.
Sub-Status	Status of the subscription.
Users	IP addresses of the phones using the shared line.

Related Commands

Command	Description
debug shared-line	Displays debugging information about SIP shared lines.

show sip dhcp

To display the Session Initiation Protocol (SIP) parameters retrieved via the Dynamic Host Configuration Protocol (DHCP), use the **show sip dhcp** command in privileged EXEC mode.

show sip dhcp

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.4(22)YB	This command was introduced.
15.0(1)M	This command was integrated in Cisco IOS Release 15.0(1)M.

Usage Guidelines

If SIP parameters are configured to be retrieved via DHCP, use the show sip dhcp command to display the SIP parameters retrieved.

Examples

The following is sample output from the show sip dhcp command:

```
Router# show sip dhcp
SIP UAC DHCP Info
SIP-DHCP interface:  GigabitEthernet0/0
SIP server address:  ipv4:9.13.2.36
Pilot number:        777777
Domain name:         dns:cisco.com
Secondary number:    222222
Secondary number:    333333
Secondary number:    444444
Secondary number:    555555
Secondary number:    666666
```

Table 1 describes the significant fields shown in the display.

Table 137: show sip dhcp Field Descriptions

Field	Description
SIP-DHCP interface	Indicates the type and number of the interface assigned to be used for SIP provisioning via DHCP.
SIP server address	Displays the address of the SIP server configured on the DHCP server and retrieved via DHCP.
Pilot number	Displays the pilot or contract number retrieved via DHCP and registered with the SIP server. Registration is done only for the pilot number.

Field	Description
Domain name	Indicates the domain name of the SIP server. The Cisco Unified Border Element will try to resolve this domain name by Domain Name System (DNS) into a routable layer 3 IP address for sending Register and Invite messages.
Secondary number	Indicates the first five secondary or additional numbers retrieved from the DHCP server. Secondary numbers are not registered with the SIP server.

Related Commands

Command	Description
debug ccsip dhcp	Displays information on SIP and DHCP interaction for debugging DHCP provisioning of SIP parameters.



show sip service through show trunk hdlc

- show sip service, on page 697
- show sip-ua calls, on page 698
- show sip-ua connections, on page 713
- show sip-ua map, on page 721
- show sip-ua min-se, on page 724
- show sip-ua mwi, on page 725
- show sip-ua register status, on page 727
- show sip-ua retry, on page 729
- show sip-ua service, on page 731
- show sip-ua srtp, on page 733
- show sip-ua statistics, on page 735
- show sip-ua status, on page 744
- show sip-ua status refer-ood, on page 748
- show sip-ua timers, on page 750
- show spe voice, on page 753
- show ss7 mtp1 channel-id, on page 756
- show ss7 mtp1 links, on page 759
- show ss7 mtp2 ccb, on page 762
- show ss7 mtp2 state, on page 765
- show ss7 mtp2 stats, on page 768
- show ss7 mtp2 timer, on page 772
- show ss7 mtp2 variant, on page 774
- show ss7 sm session, on page 776
- show ss7 sm set, on page 778
- show ss7 sm stats, on page 781
- show stcapp buffer-history, on page 783
- show stcapp device, on page 785
- show stcapp feature codes, on page 792
- show stcapp statistics, on page 796
- show subscription, on page 798
- show subscription local, on page 804
- show tbct, on page 809
- show tdm mapping, on page 810

- show tgrep neighbors, on page 812
- show translation-rule, on page 814
- show trunk group, on page 817
- show trunk hdlc, on page 821

show sip service

To display the status of SIP call service on a SIP gateway, use the **show sip service**commandin voice configuration mode.

show sip service

Syntax Description

This command has no arguments or keywords

Command Default

No default behaviors or values

Command Modes

Voice service configuration (config-voi-serv)

Command History

Release	Modification
12.3(1)	This command was introduced.

Examples

The following example displays output when SIP call service is enabled:

```
Router# show sip service
SIP Service is up
```

The following example displays output when SIP call service is shut down with the **shutdown** command:

```
Router# show sip service
SIP service is shut globally
under 'voice service voip'
```

The following example displays output when SIP call service is shut down with the **call service stop** command:

```
Router# show sip service
SIP service is shut
under 'voice service voip', 'sip' submode
```

The following example displays output when SIP call service is shut down with the **shutdown forced** command:

```
Router# show sip service
SIP service is forced shut globally
under 'voice service voip'
```

The following example displays output when SIP call service is shut down with the **call service stop forced** command:

```
Router# show sip service
SIP service is forced shut
under 'voice service voip', 'sip' submode
```

Field descriptions should be self-explanatory.

show sip-ua calls

To display active user agent client (UAC) and user agent server (UAS) information on Session Initiation Protocol (SIP) calls, use the **show sip-ua calls** command in privileged EXEC mode.

show sip-ua calls [**brief**]

Syntax Description

brief	Displays a summary of calls.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.2(15)T	This command was introduced.
12.4(22)T	Command output was updated to show IPv6 information and to display Resource Reservation Protocol (RSVP) quality of service (QoS) preconditions information.
Cisco IOS 15.6(2)T	Command output was updated to show Local UUID and Remote UUID information.
Cisco IOS XE Everest 16.5.1b	Command output was updated to show AEAD_AES_256_GCM and AEAD_AES_128_GCM cipher suites under Local Crypto Suite and Remote Crypto Suite.
Cisco IOS XE Release 16.11.1	Command output was updated to show Local Crypto Key and Remote Crypto Key.
Cisco IOS XE Bengaluru 17.6.1a	This command was enhanced to include information on fields related to WebSocket calls.

Usage Guidelines

The **show sip-ua calls** command displays active UAC and UAS information for SIP calls on a Cisco IOS device. The output includes information about IPv6, RSVP, and media forking for each call on the device and for all media streams associated with the calls. There can be any number of media streams associated with a call, of which typically only one is active. However, a call can include up to three active media streams if the call is media-forked. Use this command when debugging multiple media streams to determine if an active call on the device is forked.

From Cisco IOS XE Bengaluru 17.6.1a, this command was enhanced to include the following fields relevant to WebSocket calls:

- fork session id
- near-end channel ID (CVP side)
- far-end channel ID (CUBE side)

Note Fields corresponding to QoS negotiation in the output produced by the **show sip-ua calls** command should be ignored when the CUBE is not configured with RSVP.

```
Local QoS Strength : BestEffort
Negotiated QoS Strength : BestEffort
Negotiated QoS Direction : None
```

Note If you are using Cisco IOS XE Denali 16.3.6, 16.3.7, or 16.3.8, we recommend that you upgrade to Cisco IOS XE Everest 16.06.05, 16.06.06, or Cisco IOS XE Fuji 16.09.03 to see the correct details in the *Media Dest IP Addr:Port* and *RmtMediaIP* fields.

The following is sample output from the **show sip-ua calls** command for a call forked with WebSocket connection:

```
router# show sip-ua calls
Total SIP call legs:2, User Agent Client:1, User Agent Server:1
SIP UAC CALL INFO
Call 1
SIP Call ID : 382AC8C3-CF1611EA-80229C76-5A10D8B5@10.64.86.201
State of the call : STATE_ACTIVE (7)
Substate of the call : SUBSTATE_NONE (0)
Calling Number : 808808
Called Number : 5555
Called URI : sip:5555@10.64.86.70:8071
Bit Flags : 0xC04018 0x90000100 0x80
CC Call ID : 24
Local UUID : 87f5a958859a5067ba927188cfe38eac
Remote UUID : 224a1be49f0059e69ab10a29d7956345
Source IP Address (Sig ): 10.64.86.201
Destn SIP Req Addr:Port : [10.64.86.70]:8071
Destn SIP Resp Addr:Port: [10.64.86.70]:8071
Destination Name : 10.64.86.70
Number of Media Streams : 1
Number of Active Streams: 1
RTP Fork Object : 0x0
Media Mode : flow-through
Media Stream 1
State of the stream : STREAM_ACTIVE
Stream Call ID : 24
Stream Type : voice-only (0)
Stream Media Addr Type : 1
Negotiated Codec : g711alaw (160 bytes)
Codec Payload Type : 8
Negotiated Dtmf-relay : inband-voice
Dtmf-relay Payload Type : 0
QoS ID : -1
Local QoS Strength : BestEffort
Negotiated QoS Strength : BestEffort
Negotiated QoS Direction : None
Local QoS Status : None
Media Source IP Addr:Port: [10.64.86.201]:8006
Media Dest IP Addr:Port : [10.64.86.70]:6021
Mid-Call Re-Assocation Count: 0
SRTP-RTP Re-Assocation DSP Query Count: 0
```

```
Fork session id: 2
Near-end channel id: 3
Far-end channel id: 4


Options-Ping ENABLED:NO ACTIVE:NO
Number of SIP User Agent Client(UAC) calls: 1

SIP UAS CALL INFO
Call 1
SIP Call ID : 1-14135@10.64.86.70
State of the call : STATE_ACTIVE (7)
Substate of the call : SUBSTATE_NONE (0)
Calling Number : 808808
Called Number : 5555
Called URI : sip:5555@CUBE.com
Bit Flags : 0xC0401C 0x10000100 0x4
CC Call ID : 23
Local UUID : 224a1be49f0059e69ab10a29d7956345
Remote UUID : 87f5a958859a5067ba927188cfe38eac
Source IP Address (Sig ): 10.64.86.201
Destn SIP Req Addr:Port : [10.64.86.70]:5064
Destn SIP Resp Addr:Port: [10.64.86.70]:5064
Destination Name : 10.64.86.70
Number of Media Streams : 1
Number of Active Streams: 1
RTP Fork Object : 0x0
Media Mode : flow-through
Media Stream 1
State of the stream : STREAM_ACTIVE
Stream Call ID : 23
Stream Type : voice-only (0)
Stream Media Addr Type : 1
Negotiated Codec : g711alaw (160 bytes)
Codec Payload Type : 8
Negotiated Dtmf-relay : inband-voice
Dtmf-relay Payload Type : 0
QoS ID : -1
Local QoS Strength : BestEffort
Negotiated QoS Strength : BestEffort
Negotiated QoS Direction : None
Local QoS Status : None
Media Source IP Addr:Port: [10.64.86.201]:8004
Media Dest IP Addr:Port : [10.64.86.70]:6024
Mid-Call Re-Assocation Count: 0
SRTP-RTP Re-Assocation DSP Query Count: 0


Options-Ping ENABLED:NO ACTIVE:NO
Number of SIP User Agent Server(UAS) calls: 1
```

The following is sample output from the **show sip-ua calls** command for a forked call with four associated media streams, three of which are currently active:

```
Device# show sip-ua calls
SIP UAC CALL INFO
Call 1
SIP Call ID : 515205D4-20B711D6-8015FF77-1973C402@172.18.195.49
State of the call : STATE_ACTIVE (6)
Substate of the call : SUBSTATE_NONE (0)
Calling Number : 5550200
Called Number : 5551101
Bit Flags : 0x12120030 0x220000
```

```
Source IP Address (Sig ): 172.18.195.49
Destn SIP Req Addr:Port : 172.18.207.18:5063
Destn SIP Resp Addr:Port: 172.18.207.18:5063
Destination Name : 172.18.207.18
Number of Media Streams : 4
Number of Active Streams: 3
RTP Fork Object : 0x637C7B60
Media Stream 1
State of the stream : STREAM_ACTIVE
Stream Call ID : 28
Stream Type : voice-only (0)
Negotiated Codec : g711ulaw (160 bytes)
Codec Payload Type : 0
Negotiated Dtmf-relay : inband-voice
Dtmf-relay Payload Type : 0
Media Source IP Addr:Port: 172.18.195.49:19444
Media Dest IP Addr:Port : 172.18.193.190:16890
Media Stream 2
State of the stream : STREAM_ACTIVE
Stream Call ID : 33
Stream Type : voice+dtmf (1)
Negotiated Codec : g711ulaw (160 bytes)
Codec Payload Type : 0
Negotiated Dtmf-relay : rtp-nte
Dtmf-relay Payload Type : 101
Media Source IP Addr:Port: 172.18.195.49:18928
Media Dest IP Addr:Port : 172.18.195.73:18246
Media Stream 3
State of the stream : STREAM_ACTIVE
Stream Call ID : 34
Stream Type : dtmf-only (2)
Negotiated Codec : No Codec (0 bytes)
Codec Payload Type : -1 (None)
Negotiated Dtmf-relay : rtp-nte
Dtmf-relay Payload Type : 101
Media Source IP Addr:Port: 172.18.195.49:18428
Media Dest IP Addr:Port : 172.16.123.99:34463
Media Stream 4
State of the stream : STREAM_DEAD
Stream Call ID : -1
Stream Type : dtmf-only (2)
Negotiated Codec : No Codec (0 bytes)
Codec Payload Type : -1 (None)
Negotiated Dtmf-relay : rtp-nte
Dtmf-relay Payload Type : 101
Media Source IP Addr:Port: 172.18.195.49:0
Media Dest IP Addr:Port : 172.16.123.99:0
Number of UAC calls: 1
SIP UAS CALL INFO
```

The following is sample output from the **show sip-ua calls** command showing IPv6 information:

```
Device# show sip-ua calls
SIP UAC CALL INFO
Call 1
SIP Call ID                : 8368ED08-1C2A11DD-80078908-BA2972D0@2001::21B:D4FF:FED7:B000
   State of the call       : STATE_ACTIVE (7)
   Substate of the call    : SUBSTATE_NONE (0)
   Calling Number          : 2000
   Called Number           : 1000
   Bit Flags               : 0xC04018 0x100 0x0
   CC Call ID              : 2
   Source IP Address (Sig ): 2001::21B:D4FF:FED7:B000
   Destn SIP Req Addr:Port : [2001::21B:D5FF:FE1D:6C00]:5060
```

```
   Destn SIP Resp Addr:Port: [2001::21B:D5FF:FE1D:6C00]:5060
   Destination Name        : 2001::21B:D5FF:FE1D:6C00
   Number of Media Streams : 1
   Number of Active Streams: 1
   RTP Fork Object         : 0x0
   Media Mode              : flow-through
   Media Stream 1
     State of the stream      : STREAM_ACTIVE
     Stream Call ID           : 2
     Stream Type              : voice-only (0)
     Stream Media Addr Type   : 1709707780
     Negotiated Codec         :  (20 bytes)
     Codec Payload Type       : 18
     Negotiated Dtmf-relay    : inband-voice
     Dtmf-relay Payload Type  : 0
     Media Source IP Addr:Port: [2001::21B:D4FF:FED7:B000]:16504
     Media Dest IP Addr:Port  : [2001::21B:D5FF:FE1D:6C00]:19548
Options-Ping    ENABLED:NO    ACTIVE:NO
   Number of SIP User Agent Client(UAC) calls: 1
SIP UAS CALL INFO
   Number of SIP User Agent Server(UAS) calls: 0
```

The following is sample output from the **show sip-ua calls** command when mandatory QoS is configured at both endpoints and RSVP has succeeded:

```
Device# show sip-ua calls
SIP UAC CALL INFO
  Number of SIP User Agent Client(UAC) calls: 0
SIP UAS CALL INFO
Call 1
SIP Call ID              : F31FEA20-CFF411DC-8068DDB4-22C622B8@172.18.19.73
 State of the call       : STATE_ACTIVE (7)
 Substate of the call    : SUBSTATE_NONE (0)
 Calling Number          : 6001
 Called Number           : 1001
 Bit Flags               : 0x8C4401E 0x100 0x4
 CC Call ID              : 30
 Source IP Address (Sig ): 172.18.19.72
 Destn SIP Req Addr:Port : 172.18.19.73:5060
 Destn SIP Resp Addr:Port: 172.18.19.73:64440
 Destination Name        : 172.18.19.73
 Number of Media Streams : 1
 Number of Active Streams: 1
 RTP Fork Object         : 0x0
 Media Mode              : flow-through
 Media Stream 1
  State of the stream      : STREAM_ACTIVE
  Stream Call ID           : 30
  Stream Type              : voice-only (0)
  Negotiated Codec         : g711ulaw (160 bytes)
  Codec Payload Type       : 0
  Negotiated Dtmf-relay    : inband-voice
  Dtmf-relay Payload Type  : 0
  Media Source IP Addr:Port: 172.18.19.72:18542
  Media Dest IP Addr:Port  : 172.18.19.73:16912
  Orig Media Dest IP Addr:Port : 0.0.0.0:0
  QoS ID                   : -2
  Local QoS Strength       : Mandatory
  Negotiated QoS Strength  : Mandatory
  Negotiated QoS Direction : SendRecv
  Local QoS Status         : Success
Options-Ping    ENABLED:NO     ACTIVE:NO
```

```
 Number of SIP User Agent Server(UAS) calls: 1
```

The following is sample output from the **show sip-ua calls** command when optional QoS is configured at both endpoints and RSVP has succeeded:

```
Device# show sip-ua calls
SIP UAC CALL INFO

   Number of SIP User Agent Client(UAC) calls: 0

SIP UAS CALL INFO

Call 1
SIP Call ID              : 867EA226-D01311DC-8041CA97-F9A5F4F1@172.18.19.73
 State of the call       : STATE_ACTIVE (7)
 Substate of the call    : SUBSTATE_NONE (0)
 Calling Number          : 6001
 Called Number           : 1001
 Bit Flags               : 0x8C4401E 0x100 0x4
 CC Call ID              : 30
 Source IP Address (Sig ): 172.18.19.72
 Destn SIP Req Addr:Port : 172.18.19.73:5060
 Destn SIP Resp Addr:Port: 172.18.19.73:25055
 Destination Name        : 172.18.19.73
 Number of Media Streams : 1
 Number of Active Streams: 1
 RTP Fork Object         : 0x0
 Media Mode              : flow-through
 Media Stream 1
  State of the stream      : STREAM_ACTIVE
  Stream Call ID           : 30
  Stream Type              : voice-only (0)
  Negotiated Codec         : g711ulaw (160 bytes)
  Codec Payload Type       : 0
  Negotiated Dtmf-relay    : inband-voice
  Dtmf-relay Payload Type  : 0
  Media Source IP Addr:Port: 172.18.19.72:17556
  Media Dest IP Addr:Port  : 172.18.19.73:17966
  Orig Media Dest IP Addr:Port : 0.0.0.0:0
  QoS ID                   : -2
  Local QoS Strength       : Optional
  Negotiated QoS Strength  : Optional
  Negotiated QoS Direction : SendRecv
  Local QoS Status         : Success
Options-Ping    ENABLED:NO    ACTIVE:NO
   Number of SIP User Agent Server(UAS) calls: 1
```

The following is sample output from the **show sip-ua calls** command when optional QoS is configured at both endpoints and RSVP has failed:

```
Device# show sip-ua calls
SIP UAC CALL INFO

   Number of SIP User Agent Client(UAC) calls: 0

SIP UAS CALL INFO

Call 1
SIP Call ID              : 867EA226-D01311DC-8041CA97-F9A5F4F1@172.18.19.73
 State of the call       : STATE_ACTIVE (7)
 Substate of the call    : SUBSTATE_NONE (0)
```

```
 Calling Number          : 6001
 Called Number           : 1001
 Bit Flags               : 0x8C4401E 0x100 0x4
 CC Call ID              : 30
 Source IP Address (Sig ): 172.18.19.72
 Destn SIP Req Addr:Port : 172.18.19.73:5060
 Destn SIP Resp Addr:Port: 172.18.19.73:25055
 Destination Name        : 172.18.19.73
 Number of Media Streams : 1
 Number of Active Streams: 1
 RTP Fork Object         : 0x0
 Media Mode              : flow-through
 Media Stream 1
  State of the stream      : STREAM_ACTIVE
  Stream Call ID           : 30
  Stream Type              : voice-only (0)
  Negotiated Codec         : g711ulaw (160 bytes)
  Codec Payload Type       : 0
  Negotiated Dtmf-relay    : inband-voice
  Dtmf-relay Payload Type  : 0
  Media Source IP Addr:Port: 172.18.19.72:17556
  Media Dest IP Addr:Port  : 172.18.19.73:17966
  Orig Media Dest IP Addr:Port : 0.0.0.0:0
  QoS ID                   : -2
  Local QoS Strength       : Optional
  Negotiated QoS Strength  : Optional
  Negotiated QoS Direction : SendRecv
  Local QoS Status         : Fail
Options-Ping    ENABLED:NO    ACTIVE:NO
   Number of SIP User Agent Server(UAS) calls: 1
```

The following is sample output from the **show sip-ua calls** command when the command is used on the originating gateway (OGW) while optional QoS is configured on the OGW, mandatory QoS is configured on the terminating gateway (TGW), and RSVP has succeeded:

```
Device# show sip-ua calls
SIP UAC CALL INFO

   Number of SIP User Agent Client(UAC) calls: 0

SIP UAS CALL INFO

Call 1
SIP Call ID              : 867EA226-D01311DC-8041CA97-F9A5F4F1@172.18.19.73
 State of the call       : STATE_ACTIVE (7)
 Substate of the call    : SUBSTATE_NONE (0)
 Calling Number          : 6001
 Called Number           : 1001
 Bit Flags               : 0x8C4401E 0x100 0x4
 CC Call ID              : 30
 Source IP Address (Sig ): 172.18.19.72
 Destn SIP Req Addr:Port : 172.18.19.73:5060
 Destn SIP Resp Addr:Port: 172.18.19.73:25055
 Destination Name        : 172.18.19.73
 Number of Media Streams : 1
 Number of Active Streams: 1
 RTP Fork Object         : 0x0
 Media Mode              : flow-through
 Media Stream 1
  State of the stream      : STREAM_ACTIVE
  Stream Call ID           : 30
  Stream Type              : voice-only (0)
```

```
  Negotiated Codec         : g711ulaw (160 bytes)
  Codec Payload Type       : 0
  Negotiated Dtmf-relay    : inband-voice
  Dtmf-relay Payload Type  : 0
  Media Source IP Addr:Port: 172.18.19.72:17556
  Media Dest IP Addr:Port  : 172.18.19.73:17966
  Orig Media Dest IP Addr:Port : 0.0.0.0:0
  QoS ID                   : -2
  Local QoS Strength       : Optional
  Negotiated QoS Strength  : Mandatory
  Negotiated QoS Direction : SendRecv
  Local QoS Status         : Success
Options-Ping    ENABLED:NO    ACTIVE:NO
   Number of SIP User Agent Server(UAS) calls: 1
```

The following is sample output from **show sip-ua calls** command showing Local UUID and Remote UUID:

```
Device# show sip-ua calls
Total SIP call legs:2, User Agent Client:1, User Agent Server:1
SIP UAC CALL INFO
Call 1
SIP Call ID                : B0965CA5-B83311E5-800DFB70-CD24AE29@10.64.86.130
   State of the call       : STATE_ACTIVE (7)
   Substate of the call    : SUBSTATE_NONE (0)
   Calling Number          : sipp
   Called Number           : 56789
   Called URI              : sip:56789@10.64.86.70:8678
   Bit Flags               : 0xC04018 0x90000100 0x0
   CC Call ID              : 3
   Local UUID              : db248b6cbdc547bbc6c6fdfb6916eeb
   Remote UUID             : 4fd24d9121935531a7f8d750ad16e19
   Source IP Address (Sig ): 10.64.86.130
   Destn SIP Req Addr:Port : [10.64.86.70]:8678
   Destn SIP Resp Addr:Port: [10.64.86.70]:8678
   Destination Name        : 10.64.86.70
   Number of Media Streams : 1
   Number of Active Streams: 1
   RTP Fork Object         : 0x0
   Media Mode              : flow-through
   Media Stream 1
     State of the stream      : STREAM_ACTIVE
     Stream Call ID           : 3
     Stream Type              : voice-only (0)
     Stream Media Addr Type   : 1
     Negotiated Codec         : g711ulaw (160 bytes)
     Codec Payload Type       : 0
     Negotiated Dtmf-relay    : inband-voice
     Dtmf-relay Payload Type  : 0
     QoS ID                   : -1
     Local QoS Strength       : BestEffort
     Negotiated QoS Strength  : BestEffort
     Negotiated QoS Direction : None
     Local QoS Status         : None
     Media Source IP Addr:Port: [10.64.86.130]:16388
     Media Dest IP Addr:Port  : [9.45.33.11]:16384


Options-Ping    ENABLED:NO    ACTIVE:NO
   Number of SIP User Agent Client(UAC) calls: 1

SIP UAS CALL INFO
```

```
Call 1
SIP Call ID                : 1-22408@10.64.86.70
   State of the call       : STATE_SENT_SUCCESS (15)
   Substate of the call    : SUBSTATE_NONE (0)
   Calling Number          : sipp
   Called Number           : 56789
   Called URI              : sip:56789@10.64.86.130:5060
   Bit Flags               : 0xC0401E 0x10000100 0x200444
   CC Call ID              : 2
   Local UUID              : 4fd24d9121935531a7f8d750ad16e19
   Remote UUID             : db248b6cbdc547bbc6c6fdfb6916eeb
   Source IP Address (Sig ): 10.64.86.130
   Destn SIP Req Addr:Port : [10.64.86.70]:5061
   Destn SIP Resp Addr:Port: [10.64.86.70]:5061
   Destination Name        : 10.64.86.70
   Number of Media Streams : 1
   Number of Active Streams: 1
   RTP Fork Object         : 0x0
   Media Mode              : flow-through
   Media Stream 1
     State of the stream      : STREAM_ACTIVE
     Stream Call ID           : 2
     Stream Type              : voice-only (0)
     Stream Media Addr Type   : 1
     Negotiated Codec         : g711ulaw (160 bytes)
     Codec Payload Type       : 0
```

The following is sample output from the **show sip-ua calls** command showing AEAD_AES_256_GCM and AEAD_AES_128_GCM cipher-suites under Local Crypto Suite and Remote Crypto Suite:

```
Device# show sip-ua calls
Total SIP call legs:2, User Agent Client:1, User Agent Server:1
SIP UAC CALL INFO
Call 1
SIP Call ID                : A574C2A9-849711E6-8008B4F0-6A529C6A@8.39.16.17
   State of the call       : STATE_ACTIVE (7)
   Substate of the call    : SUBSTATE_NONE (0)
   Calling Number          : 909909
   Called Number           : 909909
   Called URI              : sip:909909@8.0.0.200:1256
   Bit Flags               : 0xC04018 0x90000100 0x0
   CC Call ID              : 2
   Local UUID              : dfe71ed9bfba5a34abd76546cfa07b81
   Remote UUID             : 06c8a6ae52fb57888aeebb588693ba2c
   Source IP Address (Sig ): 8.39.16.17
   Destn SIP Req Addr:Port : [8.0.0.200]:1256
   Destn SIP Resp Addr:Port: [8.0.0.200]:1256
   Destination Name        : 8.0.0.200
   Number of Media Streams : 1
   Number of Active Streams: 1
   RTP Fork Object         : 0x0
   Media Mode              : flow-through
   Media Stream 1
     State of the stream      : STREAM_ACTIVE
     Stream Call ID           : 2
     Stream Type              : voice+dtmf (1)
     Stream Media Addr Type   : 1
     Negotiated Codec         : g711ulaw (160 bytes)
     Codec Payload Type       : 0
     Negotiated Dtmf-relay    : rtp-nte
     Dtmf-relay Payload Type  : 101
```

```
     QoS ID                   : -1
     Local QoS Strength       : BestEffort
     Negotiated QoS Strength  : BestEffort
     Negotiated QoS Direction : None
     Local QoS Status         : None
     Media Source IP Addr:Port: [8.39.16.17]:16386
     Media Dest IP Addr:Port  : [8.0.0.200]:39768
     Local Crypto Suite       :  AEAD_AES_128_GCM(
                                 AEAD_AES_256_GCM
                                 AEAD_AES_128_GCM
                                 AES_CM_128_HMAC_SHA1_80
                                 AES_CM_128_HMAC_SHA1_32 )
     Remote Crypto Suite      :  AEAD_AES_128_GCM
     Local Crypto Key         : bTQqZXbgFJddA1hE9wJGV3aKxo5vPV+Z1234tVb2
     Remote Crypto Key        : bTQqZXbgFJddA1hE9wJGV3aKxo5vPV+Z9876tVb2
   Mid-Call Re-Assocation Count: 0
   SRTP-RTP Re-Assocation DSP Query Count: 0


Options-Ping    ENABLED:NO    ACTIVE:NO
   Number of SIP User Agent Client(UAC) calls: 1

SIP UAS CALL INFO
Call 1
SIP Call ID               : 1-25632@8.0.0.200
   State of the call      : STATE_ACTIVE (7)
   Substate of the call   : SUBSTATE_NONE (0)
   Calling Number         : 909909
   Called Number          : 909909
   Called URI             : sip:909909@8.39.16.17:5060
   Bit Flags              : 0x8C4401C 0x10000100 0x0
   CC Call ID             : 1
   Local UUID             : 06c8a6ae52fb57888aeebb588693ba2c
   Remote UUID            : dfe71ed9bfba5a34abd76546cfa07b81
   Source IP Address (Sig ): 8.39.16.17
   Destn SIP Req Addr:Port : [8.0.0.200]:7256
   Destn SIP Resp Addr:Port: [8.0.0.200]:7256
   Destination Name       : 8.0.0.200
   Number of Media Streams : 1
   Number of Active Streams: 1
   RTP Fork Object        : 0x0
   Media Mode             : flow-through
   Media Stream 1
     State of the stream      : STREAM_ACTIVE
     Stream Call ID           : 1
     Stream Type              : voice+dtmf (0)
     Stream Media Addr Type   : 1
     Negotiated Codec         : g711ulaw (160 bytes)
     Codec Payload Type       : 0
     Negotiated Dtmf-relay    : rtp-nte
     Dtmf-relay Payload Type  : 101
     QoS ID                   : -1
     Local QoS Strength       : BestEffort
     Negotiated QoS Strength  : BestEffort
     Negotiated QoS Direction : None
     Local QoS Status         : None
     Media Source IP Addr:Port: [8.39.16.17]:16384
     Media Dest IP Addr:Port  : [8.0.0.200]:39768
     Local Crypto Suite       :  AES_CM_128_HMAC_SHA1_80
     Remote Crypto Suite      :  AES_CM_128_HMAC_SHA1_80(
                                 AEAD_AES_256_GCM
                                 AEAD_AES_128_GCM
                                 AES_CM_128_HMAC_SHA1_80
                                 AES_CM_128_HMAC_SHA1_32 )
```

```
     Local Crypto Key         : bTQqZXbgFJddA1hE9wJGV3aKxo5vPV+Z1234tVb2
     Remote Crypto Key        : bTQqZXbgFJddA1hE9wJGV3aKxo5vPV+Z9876tVb2
   Mid-Call Re-Assocation Count: 0
   SRTP-RTP Re-Assocation DSP Query Count: 0


Options-Ping    ENABLED:NO    ACTIVE:NO
   Number of SIP User Agent Server(UAS) calls: 1
```

The following is sample output from the **show sip-ua calls** command showing Local Crypto Key and Remote Crypto Key:

```
Device# show sip-ua calls

Total SIP call legs:2, User Agent Client:1, User Agent Server:1
SIP UAC CALL INFO
Call 1
SIP Call ID                : C9A3AA00-B49A11E8-8018A74B-CD0B0450@10.0.0.1
   State of the call       : STATE_ACTIVE (7)
   Substate of the call    : SUBSTATE_NONE (0)
   Calling Number          : 1234
   Called Number           : 9876
   Called URI              : sip:9876@10.0.0.2:9800
   Bit Flags               : 0xC04018 0x90000100 0x80
   CC Call ID              : 13
   Local UUID              : 7d14e2d622ec504f9aaa4ba029ddd136
   Remote UUID             : 2522eaa82f505c868037da95438fc49b
   Source IP Address (Sig ): 10.0.0.1
   Destn SIP Req Addr:Port : [10.0.0.2]:9800
   Destn SIP Resp Addr:Port: [10.0.0.2]:9800
   Destination Name        : 10.0.0.1
   Number of Media Streams : 2
   Number of Active Streams: 2
   RTP Fork Object         : 0x0
   Media Mode              : flow-through
   Media Stream 1
     State of the stream      : STREAM_ACTIVE
     Stream Call ID           : 13
     Stream Type              : voice-only (0)
     Stream Media Addr Type   : 1
     Negotiated Codec         : g711ulaw (160 bytes)
     Codec Payload Type       : 0
     Negotiated Dtmf-relay    : inband-voice
     Dtmf-relay Payload Type  : 0
     QoS ID                   : -1
     Local QoS Strength       : BestEffort
     Negotiated QoS Strength  : BestEffort
     Negotiated QoS Direction : None
     Local QoS Status         : None
     Media Source IP Addr:Port: [10.0.0.1]:8022
     Media Dest IP Addr:Port  : [10.0.0.2]:6008
     Local Crypto Suite       :  AES_CM_128_HMAC_SHA1_80 (
                                 AEAD_AES_256_GCM
                                 AEAD_AES_128_GCM
                                 AES_CM_128_HMAC_SHA1_80
                                 AES_CM_128_HMAC_SHA1_32 )
     Remote Crypto Suite      :  AES_CM_128_HMAC_SHA1_80
     Local Crypto Key         : bTQqZXbgFJddA1hE9wJGV3aKxo5vPV+Z1234tVb2
     Remote Crypto Key        : bTQqZXbgFJddA1hE9wJGV3aKxo5vPV+Z9876tVb2
   Media Stream 2
     State of the stream      : STREAM_ACTIVE
     Stream Call ID           : 14
     Stream Type              : video (7)
```

```
     Stream Media Addr Type   : 1
     Negotiated Codec         : h264 (0 bytes)
     Codec Payload Type       : 97
     Negotiated Dtmf-relay    : inband-voice
     Dtmf-relay Payload Type  : 0
     QoS ID                   : -1
     Local QoS Strength       : BestEffort
     Negotiated QoS Strength  : BestEffort
     Negotiated QoS Direction : None
     Local QoS Status         : None
     Media Source IP Addr:Port: [10.0.0.1]:8020
     Media Dest IP Addr:Port  : [10.0.0.2]:9802
     Local Crypto Suite       :  AES_CM_128_HMAC_SHA1_80 (
                                 AEAD_AES_256_GCM
                                 AEAD_AES_128_GCM
                                 AES_CM_128_HMAC_SHA1_80
                                 AES_CM_128_HMAC_SHA1_32 )
     Remote Crypto Suite      :  AES_CM_128_HMAC_SHA1_80
     Local Crypto Key         : bTQqZXbgFJddA1hE9wJGV3aKxo5vPV+Z2345tVb2
     Remote Crypto Key        : bTQqZXbgFJddA1hE9wJGV3aKxo5vPV+Z8765tVb2
   Mid-Call Re-Assocation Count: 0
   SRTP-RTP Re-Assocation DSP Query Count: 0


Options-Ping    ENABLED:NO    ACTIVE:NO
   Number of SIP User Agent Client(UAC) calls: 1

SIP UAS CALL INFO
Call 1
SIP Call ID               : 1-12049@10.0.0.2
   State of the call      : STATE_ACTIVE (7)
   Substate of the call   : SUBSTATE_NONE (0)
   Calling Number         : 1234
   Called Number          : 9876
   Called URI             : sip:9876@10.0.0.1:5060
   Bit Flags              : 0xC0401C 0x10000100 0x4
   CC Call ID             : 11
   Local UUID             : 2522eaa82f505c868037da95438fc49b
   Remote UUID            : 7d14e2d622ec504f9aaa4ba029ddd136
   Source IP Address (Sig ): 10.0.0.1
   Destn SIP Req Addr:Port : [10.0.0.2]:5060
   Destn SIP Resp Addr:Port: [10.0.0.2]:5060
   Destination Name       : 10.0.0.2
   Number of Media Streams : 2
   Number of Active Streams: 2
   RTP Fork Object        : 0x0
   Media Mode             : flow-through
   Media Stream 1
     State of the stream      : STREAM_ACTIVE
     Stream Call ID           : 11
     Stream Type              : voice-only (0)
     Stream Media Addr Type   : 1
     Negotiated Codec         : g711ulaw (160 bytes)
     Codec Payload Type       : 0
     Negotiated Dtmf-relay    : inband-voice
     Dtmf-relay Payload Type  : 0
     QoS ID                   : -1
     Local QoS Strength       : BestEffort
     Negotiated QoS Strength  : BestEffort
     Negotiated QoS Direction : None
     Local QoS Status         : None
     Media Source IP Addr:Port: [10.0.0.1]:8016
     Media Dest IP Addr:Port  : [10.0.0.2]:6009
     Local Crypto Suite       :  AES_CM_128_HMAC_SHA1_80
```

```
     Remote Crypto Suite      :  AES_CM_128_HMAC_SHA1_80
     Local Crypto Key         : bTQqZXbgFJddA1hE9wJGV3aKxo5vPV+Z9876tVb2
     Remote Crypto Key        : bTQqZXbgFJddA1hE9wJGV3aKxo5vPV+Z1234tVb2
   Media Stream 2
     State of the stream      : STREAM_ACTIVE
     Stream Call ID           : 12
     Stream Type              : video (7)
     Stream Media Addr Type   : 1
     Negotiated Codec         : h264 (0 bytes)
     Codec Payload Type       : 97
     Negotiated Dtmf-relay    : inband-voice
     Dtmf-relay Payload Type  : 0
     QoS ID                   : -1
     Local QoS Strength       : BestEffort
     Negotiated QoS Strength  : BestEffort
     Negotiated QoS Direction : None
     Local QoS Status         : None
     Media Source IP Addr:Port: [10.0.0.1]:8018
     Media Dest IP Addr:Port  : [10.0.0.2]:5062
     Local Crypto Suite       :  AES_CM_128_HMAC_SHA1_80
     Remote Crypto Suite      :  AES_CM_128_HMAC_SHA1_80
     Local Crypto Key         : bTQqZXbgFJddA1hE9wJGV3aKxo5vPV+Z8765tVb2
     Remote Crypto Key        : bTQqZXbgFJddA1hE9wJGV3aKxo5vPV+Z2345tVb2
   Mid-Call Re-Assocation Count: 0
   SRTP-RTP Re-Assocation DSP Query Count: 0


Options-Ping    ENABLED:NO    ACTIVE:NO
   Number of SIP User Agent Server(UAS) calls: 1
```

The following is sample output from the **show sip-ua calls brief** command:

```
Device# show sip-ua calls brief

Total SIP call legs:2, User Agent Client:1, User Agent Server:1
SIP UAC CALL INFO
No.  CallId    Calling#       Called#        RmtSignalIP
RmtMediaIP
     dstCallId SIPState       SIPSubState
=============================================================================================================
1    2         5680           5678           10.1.76.151
10.1.99.101
     1         STATE_ACTIVE   SUBSTATE_NONE
   Number of SIP User Agent Client(UAC) calls: 1

SIP UAS CALL INFO
No.  CallId    Calling#       Called#        RmtSignalIP
RmtMediaIP
     dstCallId SIPState       SIPSubState
=============================================================================================================
1    1         5680           95678          10.1.76.151
10.1.99.199
     2         STATE_ACTIVE   SUBSTATE_NONE
   Number of SIP User Agent Server(UAS) calls: 1
```

The table below describes the significant fields shown in the displays.

Table 138: show sip-ua calls Field Descriptions

Field	Description
SIP UAC CALL INFO	Field header that indicates that the following information pertains to the SIP UAC.

Field	Description
Call 1	Field header.
SIP Call ID	UAC call identification number.
State of the call	Indicates the state of the call. This field is used for debugging purposes. The state is variable and may be different from one Cisco IOS release to another.
Substate of the call	Indicates the substate of the call. This field is used for debugging purposes. The state is variable and may be different from one Cisco IOS release to another.
Calling Number	Indicates the calling number.
Called Number	Indicates the called number.
Bit Flags	Indicates the bit flags used for debugging.
Source IP Address (Sig)	Indicates the signaling source IPv4 or IPv6 address.
Destn SIP Req Addr: Port:	Indicates the signaling destination Request IPv4 or IPv6 address and port number.
Destn SIP Resp Addr: Port:	Indicates the signaling destination Response IPv4 or IPv6 address and port number.
Destination Name	Indicates the signaling destination hostname, IPv4 address, or IPv6 address.
Number of Media Streams	Indicates the total number of media streams for this UAC call.
Number of Active Streams:	Indicates the total number of active media streams.
RTP Fork Object	Pointer address of the internal RTP Fork data structure.
Media Stream	Statistics about each active media stream are reported. The Media Stream header indicates the number of the media stream, and its statistics immediately follow this header.
State of the stream	State of the media stream indicated by the Media Stream header. Can be STREAM_ACTIVE, STREAM_ADDING, STREAM_CHANGING, STREAM_DEAD, STREAM_DELETING, STREAM_IDLE, or Invalid Stream State.
Stream Call ID	Identification of the stream call indicated by the Media Stream header.
Stream Type	Type of stream indicated by the Media Stream header. It can be dtmf-only, dtmf-relay, voice-only, or voice+dtmf-relay.
Negotiated Codec	Codec selected for the media stream. It can be g711ulaw, <G.729>, <G.726>, or No Codec.
Codec Payload Type	Payload type of the Negotiated Codec.
Negotiated Dtmf-relay	DTMF relay selected for the media stream indicated by the Media Stream header. It can be inband-voice or rtp-nte.

Field	Description
Dtmf-relay Payload Type	Payload type of the negotiated DTMF relay.
Media Source IP Addr: Port	The source IPv4 or IPv6 address and port number of the media stream indicated by the Media Stream header.
Media Dest IP Addr: Port	The destination IPv4 or IPv6 address and port number of the media stream indicated by the Media Stream header.
Local QoS Strength	The QoS strength (mandatory or optional) configured for this device.
Negotiated QoS Strength	The QoS strength (mandatory or optional) that has been negotiated.
Negotiated QoS Direction	Displays the direction in which RSVP was negotiated. For example, sendrecv indicates that RSVP was negotiated in both directions.
Local QoS Status	Displays the success or failure of RSVP reservation.
Number of UAC calls	Final SIP UAC CALL INFO field. Indicates the number of UAC calls.
SIP UAS CALL INFO	Field header that indicates that the following information pertains to the SIP UAS.
Number of UAS calls	Final SIP UAS CALL INFO field. Indicates the number of UAS calls.
Local UUID	Unique identifier generated from the originating user agent.
Remote UUID	Unique identifier generated from the terminating user agent.
Local Crypto Suite	Crypto suite negotiated by CUBE. All the crypto suites configured in CUBE are listed in parenthesis.
Remote Crypto Suite	Crypto suites received.

Related Commands

Command	Description
debug ccsip all	Enables all SIP-related debugging.
debug ccsip events	Enables tracing of events that are specific to SIP SPI.
debug ccsip info	Enables tracing of general SIP SPI information.
debug ccsip media	Enables tracing of SIP call media streams.
debug ccsip messages	Enables tracing of SIP Service Provider Interface (SPI) messages.

show sip-ua connections

To display Session Initiation Protocol (SIP) user-agent (UA) transport connection tables, use the **show sip-ua connections** command in privileged EXEC mode.

show sip-ua connections {**tcp** [**tls**] | **udp**} {**brief** | **detail**}

Syntax Description

tcp	Displays all TCP connection information.
tls	(Optional) Displays all Transport Layer Security (TLS) over TCP connection information.
udp	Displays all User Datagram Protocol (UDP) connection information.
brief	Displays a summary of connections.
detail	Displays detailed connection information.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Cupertino 17.8.1a	The command output was updated to print the tenant-tag information associated with each connection and listen socket for UDP, TCP, and TLS transport types.
Cisco IOS XE 16.10.1	The command output for **show sip-ua connections tcp tls detail** was updated to display the Cipher and the Curve-Size.
Cisco IOS XE 17.14.1a	The command output for **show sip-ua connections tcp tls detail** is updated to display TLS v1.3 cipher configurations.

Usage Guidelines

The **show sip-ua connections** command should be executed only after a call is made. Use this command to learn the connection details.

Cisco IOS XE 17.14.1a and Later Releases

Note The RSA and ECDSA key types are displayed only for TLS version 1.3 configurations.

The following is a sample output from the **show sip-ua connections tcp tls brief** command displaying "RSA" key type along with TLS v1.3 ciphers:

```
Device# show sip-ua connections tcp tls detail
Total active connections      : 2
No. of send failures          : 0
No. of remote closures        : 0
No. of conn. failures         : 0
No. of inactive conn. ageouts : 0
Max. tls send msg queue size of 1, recorded for 10.64.100.152:5061
TLS client handshake failures : 0
```

```
TLS server handshake failures : 0

---------Printing Detailed Connection Report---------
Note:
 ** Tuples with no matching socket entry
    - Do 'clear sip <tcp[tls]/udp> conn t ipv4:<addr>:<port>'
      to overcome this error condition
 ++ Tuples with mismatched address/port entry
    - Do 'clear sip <tcp[tls]/udp> conn t ipv4:<addr>:<port> id <connid>'
      to overcome this error condition
 * Connections with SIP OAuth ports

Remote-Agent:10.64.100.150, Connections-Count:1
  Remote-Port Conn-Id Conn-State  WriteQ-Size            Local-Address
TLS-Version                Cipher              Curve Tenant
  =========== ======= =========== =========== ====================================
=========== ================================== ===== ======
        22943       7 Established           0 10.64.100.151:5061
TLSv1.3         TLS_AES_256_GCM_SHA384:RSA P-521     0

Remote-Agent:10.64.100.152, Connections-Count:1
  Remote-Port Conn-Id Conn-State  WriteQ-Size            Local-Address
TLS-Version                Cipher              Curve Tenant
  =========== ======= =========== =========== ====================================
=========== ================================== ===== ======
         5061       8 Established           0 10.64.100.151:47687
TLSv1.3         TLS_AES_256_GCM_SHA384:RSA P-521     0


-------------- SIP Transport Layer Listen Sockets ---------------
  Conn-Id             Local-Address                      Tenant
 ==========    ==========================             ========
  0             [0.0.0.0]:5061:                            0
  6             [10.64.100.151]:5061:                      0
```

The following is a sample output from the **show sip-ua connections tcp tls detail** command displaying "ECDSA" key type along with TLS v1.3 ciphers:

```
Device# show sip-ua connections tcp tls detail
Total active connections      : 2
No. of send failures          : 0
No. of remote closures        : 0
No. of conn. failures         : 0
No. of inactive conn. ageouts : 0
Max. tls send msg queue size of 1, recorded for 10.1.10.50:5061
TLS client handshake failures : 0
TLS server handshake failures : 0

---------Printing Detailed Connection Report---------
Note:
 ** Tuples with no matching socket entry
    - Do 'clear sip <tcp[tls]/udp> conn t ipv4:<addr>:<port>'
      to overcome this error condition
 ++ Tuples with mismatched address/port entry
    - Do 'clear sip <tcp[tls]/udp> conn t ipv4:<addr>:<port> id <connid>'
      to overcome this error condition
 * Connections with SIP OAuth ports

Remote-Agent:10.1.10.50, Connections-Count:2
  Remote-Port Conn-Id Conn-State  WriteQ-Size            Local-Address
TLS-Version               Cipher              Curve Tenant
  =========== ======= =========== =========== ====================================
=========== ================================== ===== ======
```

```
         5061       9 Established           0 10.1.20.155:37081
TLSv1.3  ECDHE-RSA-AES256-GCM-SHA384:ECDSA P-521     0
        41635       8 Established           0 10.1.20.155:5061
TLSv1.3       TLS_AES_256_GCM_SHA384:ECDSA P-256     0

  Remote-Port Conn-Id Conn-State  WriteQ-Size            Local-Address
TLS-Version Cipher                         Curve Tenant
  =========== ======= =========== =========== ======================================
========== ============================== ===== ======
        53516     102 Established           0 10.64.100.150:5061
TLSv1.2    ECDHE-RSA-AES256-GCM-SHA384 P-521     0



-------------- SIP Transport Layer Listen Sockets ---------------
  Conn-Id             Local-Address                     Tenant
 ==========    ==========================             ========
  0             [0.0.0.0]:5061:                            0
  1             [::]:5061:                                 0
  6             [10.1.20.155]:5061:                        0
  7             [2001:10:1:20::135]:5061:                  0
```

Cisco IOS XE Cupertino 17.8.1a and Later Releases

The following is a sample output from the **show sip-ua connections tcp tls brief** command showing a brief summary including the associated tenant-tag for listen sockets added in Cisco IOS XE Cupertino 17.8.1a.

```
router# show sip-ua connections tcp tls brief
Total active connections : 2
No. of send failures : 0
No. of remote closures : 47
No. of conn. failures : 43
No. of inactive conn. ageouts : 0
Max. tls send msg queue size of 1, recorded for 10.105.34.88:5061
TLS client handshake failures : 0
TLS server handshake failures : 4

-------------- SIP Transport Layer Listen Sockets ---------------
Conn-Id  Local-Address   Tenant
=========== ============================== ============
 3              [10.64.86.181]:3000:        1
19              [8.43.21.58]:4000:          2
90              [10.64.86.181]:5061:        0
```

The following is a sample output from the **show sip-ua connections tcp tls detail** command showing a connection details, including the associated tenant tag for listen sockets added in Cisco IOS XE Cupertino 17.8.1a.

```
Router#sh sip-ua connections tcp tls detail
Total active connections      : 2
No. of send failures          : 0
No. of remote closures        : 3
No. of conn. failures         : 0
No. of inactive conn. ageouts : 0
Max. tls send msg queue size of 1, recorded for 10.105.34.88:8090
TLS client handshake failures : 0
TLS server handshake failures : 0

---------Printing Detailed Connection Report---------
Note:
 ** Tuples with no matching socket entry
```

```
    - Do 'clear sip <tcp[tls]/udp> conn t ipv4:<addr>:<port>'
      to overcome this error condition
 ++ Tuples with mismatched address/port entry
    - Do 'clear sip <tcp[tls]/udp> conn t ipv4:<addr>:<port> id <connid>'
      to overcome this error condition

Remote-Agent:10.105.34.88, Connections-Count:2
  Remote-Port Conn-Id Conn-State  WriteQ-Size Local-Address TLS-Version (contd.)
  =========== ======= =========== =========== ============= ===========
        38928       9 Established           0 10.64.100.145     TLSv1.2
         8090      10 Established           0 10.64.100.145     TLSv1.2


  Cipher                        Curve       Tenant
  ============================  =========== ======
   ECDHE-RSA-AES256-GCM-SHA384        P-256     10
                    AES256-SHA                 10

-------------- SIP Transport Layer Listen Sockets ---------------
  Conn-Id             Local-Address                      Tenant
 ==========    ==========================             ========
  2             [8.43.21.8]:5061:                           0
  3             [10.64.100.145]:5090:                      10
  4             [10.64.100.145]:8123:                      50
  5             [10.64.100.145]:5061:                       0
```

The following is a sample output from the **show sip-ua connections tcp brief** command showing a summary including that prints the associated tenant-tag for listen sockets added in Cisco IOS XE Cupertino 17.8.1a.

```
CSR#sh sip-ua connections tcp brief
Total active connections      : 0
No. of send failures          : 0
No. of remote closures        : 2
No. of conn. failures         : 0
No. of inactive conn. ageouts : 0
Max. tcp send msg queue size of 1, recorded for 10.105.34.88:8091

-------------- SIP Transport Layer Listen Sockets ---------------
  Conn-Id             Local-Address                      Tenant
 ==========    ==========================             ========
  2             [8.43.21.8]:5060:                           0
  3             [10.64.100.145]:5430:                       1
  4             [10.64.100.145]:5160:                       3
  5             [10.64.100.145]:5267:                       6
```

The following is a sample output from the **show sip-ua connections tcp detail** command showing a connection details, including the associated tenant tag for listen sockets added in Cisco IOS XE Cupertino 17.8.1a.

```
Router#show sip-ua connections tcp tls detail
Total active connections      : 4
No. of send failures          : 0
No. of remote closures        : 8
No. of conn. failures         : 0
No. of inactive conn. ageouts : 0
TLS client handshake failures : 0
TLS server handshake failures : 0

---------Printing Detailed Connection Report---------
Note:
 ** Tuples with no matching socket entry
    - Do 'clear sip <tcp[tls]/udp> conn t ipv4:<addr>:<port>'
      to overcome this error condition
```

```
 ++ Tuples with mismatched address/port entry
    - Do 'clear sip <tcp[tls]/udp> conn t ipv4:<addr>:<port> id <connid>'
      to overcome this error condition
 * Connections with SIP OAuth ports

Remote-Agent:10.5.10.200, Connections-Count:0

Remote-Agent:10.5.10.201, Connections-Count:0

Remote-Agent:10.5.10.202, Connections-Count:0

Remote-Agent:10.5.10.212, Connections-Count:1
  Remote-Port Conn-Id Conn-State  WriteQ-Size Local-Address TLS-Version Cipher
              Curve
  =========== ======= =========== =========== ============= ===========
================================ =====
        52248      27 Established           0             -      TLSv1.2
ECDHE-RSA-AES256-GCM-SHA384 P-256

Remote-Agent:10.5.10.213, Connections-Count:1
  Remote-Port Conn-Id Conn-State  WriteQ-Size Local-Address TLS-Version Cipher
              Curve
  =========== ======= =========== =========== ============= ===========
================================ =====
        50901     28* Established           0             -      TLSv1.2
ECDHE-RSA-AES256-GCM-SHA384 P-256

Remote-Agent:10.5.10.209, Connections-Count:1
  Remote-Port Conn-Id Conn-State  WriteQ-Size Local-Address TLS-Version Cipher
              Curve
  =========== ======= =========== =========== ============= ===========
================================ =====
        51402     29* Established           0             -      TLSv1.2
ECDHE-RSA-AES256-GCM-SHA384 P-256

Remote-Agent:10.5.10.204, Connections-Count:1
  Remote-Port Conn-Id Conn-State  WriteQ-Size Local-Address TLS-Version Cipher
              Curve
  =========== ======= =========== =========== ============= ===========
================================ =====
        50757     30* Established           0             -      TLSv1.2
ECDHE-RSA-AES256-GCM-SHA384 P-256

Remote-Agent:10.5.10.218, Connections-Count:0


-------------- SIP Transport Layer Listen Sockets ---------------
  Conn-Id               Local-Address
 ===========    ============================
   0            [0.0.0.0]:5061:
   2            [0.0.0.0]:5090:
gw1-2a#
=================================

gw1-2a#show sip status registrar
Line          destination                              expires(sec)  contact
transport     call-id
              peer
=============================================================================================================
2999904       10.5.10.204                               76            10.5.10.204

TLS*           00451d86-f1520107-5b4fd894-7ab6c4ce@10.5.10.204
              40004
```

```
2999901       10.5.10.212                                74            10.5.10.212

TLS            00af1f9c-12dc037b-14a5f99d-09f10ac4@10.5.10.212
              40001

2999902       10.5.10.213                                75            10.5.10.213

TLS*           00af1f9c-48370020-2bf6ccd4-2423aff8@10.5.10.213
              40002

2999905       10.5.10.209                                76            10.5.10.209

TLS*           5006ab80-69ca0049-1ce700d8-12edb829@10.5.10.209
              40003
```

The following is a sample output from the **show sip-ua connections udp brief** command showing a summary including that prints the associated tenant-tag for listen sockets added in Cisco IOS XE Cupertino 17.8.1a.

```
CSR#sh sip-ua connections udp brief
Total active connections      : 0
No. of send failures          : 0
No. of remote closures        : 0
No. of conn. failures         : 0
No. of inactive conn. ageouts : 0

-------------- SIP Transport Layer Listen Sockets ---------------
  Conn-Id              Local-Address                      Tenant
 ==========    ==========================             ========
  2              [8.43.21.8]:5060:                          0
  3              [10.64.100.145]:5260:                     10
  4              [10.64.100.145]:5330:                     50
  5              [10.64.100.145]:5060:                      0
```

The following is a sample output from the **show sip-ua connections udp detail** command showing a connection details, including the associated tenant tag for listen sockets added in Cisco IOS XE Cupertino 17.8.1a.

```
CSR#sh sip-ua connections udp detail
Total active connections      : 2
No. of send failures          : 0
No. of remote closures        : 0
No. of conn. failures         : 0
No. of inactive conn. ageouts : 0

---------Printing Detailed Connection Report---------
Note:
 ** Tuples with no matching socket entry
    - Do 'clear sip <tcp[tls]/udp> conn t ipv4:<addr>:<port>'
      to overcome this error condition
 ++ Tuples with mismatched address/port entry
    - Do 'clear sip <tcp[tls]/udp> conn t ipv4:<addr>:<port> id <connid>'
      to overcome this error condition

Remote-Agent:10.105.34.88, Connections-Count:2
  Remote-Port Conn-Id Conn-State  WriteQ-Size Local-Address Tenant
  =========== ======= =========== =========== ============= ======
         5061       6 Established           0 10.64.100.145   200
         8091       7 Established           0 10.64.100.145   200


-------------- SIP Transport Layer Listen Sockets ---------------
  Conn-Id              Local-Address                      Tenant
 ==========    ==========================             ========
```

```
2               [8.43.21.8]:5060:                          0
3               [10.64.100.145]:5361:                     10
4               [10.64.100.145]:5326:                     50
5               [10.64.100.145]:5060:                    200
```

Examples

The table below describes the significant fields that are shown in the display.

Table 139: show sip-ua connections Field Descriptions

Field	Description
Total active connections	Indicates all the connections that the gateway holds for various targets. Statistics are broken down within individual fields.
No. of send failures.	Indicates the number of TCP or UDP messages dropped by the transport layer. Messages are dropped if there were network issues, and the connection was frequently ended.
No. of remote closures	Indicates the number of times a remote gateway ended the connection. A higher value indicates a problem with the network or that the remote gateway does not support reusing the connections (thus it is not RFC 3261-compliant). The remote closure number can also contribute to the number of send failures.
No. of conn. failures	Indicates the number of times that the transport layer was unsuccessful in establishing the connection to the remote agent. The field can also indicate that the address or port that is configured under the dial peer might be incorrect or that the remote gateway does not support that mode of transport.
No. of inactive conn. ageouts	Indicates the number of times that the connections were ended or timed out because of signaling inactivity. During call traffic, this number should be zero. If it is not zero, we recommend that the inactivity timer be tuned to optimize performance by using the **timers** command.
Max. tcp send msg queue size of 0, recorded for 0.0.0.0:0	Indicates the number of messages waiting in the queue to be sent out on the TCP connection when the congestion was at its peak. A higher queue number indicates that more messages are waiting to be sent on the network. The growth of this queue size cannot be controlled directly by the administrator.
Tuples with no matching socket entry	Any tuples for the connection entry that are marked with "**" at the end of the line indicate an upper transport layer error condition; specifically, that the upper transport layer is out of sync with the lower connection layer. Cisco IOS Software should automatically overcome this condition. If the error persists, execute the **clear sip-ua udp connection** or **clear sip-ua tcp connection**command and report the problem to your support team.
Tuples with mismatched address/port entry	Any tuples for the connection entry that are marked with "++" at the end of the line indicate an upper transport layer error condition, where the socket is probably readable, but is not being used. If the error persists, execute the **clear sip-ua udp connection** or **clear sip-ua tcp connection**command and report the problem to your support team.
Remote-Agent Connections-Count	Connections to the same target address. This field indicates how many connections are established to the same host.

Field	Description
Remote-Port Conn-Id Conn-State WriteQ-Size	Connections to the same target address. This field indicates how many connections are established to the same host. The WriteQ-Size field is relevant only to TCP connections and is a good indicator of network congestion and if there is a need to tune the TCP parameters.
Cipher	Displays the negotiated Cipher.
Curve	Curve Size of the ECDSA Cipher.

Related Commands

Command	Description
clear sip-ua tcp tls connection id	Clears a SIP TCP TLS connection.
clear sip-ua tcp connection	Clears a SIP TCP connection.
clear sip-ua udp connection	Clears a SIP UDP connection.
show sip-ua retry	Displays SIP retry statistics.
show sip-ua statistics	Displays response, traffic, and retry SIP statistics.
show sip-ua status	Displays SIP user agent status.
show sip-ua timers	Displays the current settings for the SIP UA timers.
sip-ua	Enables the SIP user-agent configuration commands.
timers	Configures the SIP signaling timers.

show sip-ua map

To display the mapping table of public switched telephone network (PSTN) cause codes and their corresponding Session Initiation Protocol (SIP) error status codes or the mapping table of SIP-to-PSTN codes, use the **show sip-ua map** command in privileged EXEC mode.

show sip-ua map {**pstn-sip** | **sip-pstn** | **sip-request-pstn**}

Syntax Description

pstn-sip	Displays the PSTN cause-code-to-SIP-status-code mapping table.
sip-pstn	Displays the SIP-status-code-to-PSTN-cause-code mapping table.
sip-request-pstn	Display the SIP-requests-PSTN-cause mapping table.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.2(2)XB	This command was introduced.
12.2(2)XB2	This command was implemented on the Cisco AS5850.
12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T. Support for the Cisco AS5300, Cisco AS5350, Cisco AS5400, and Cisco AS5850 was not included in this release.
12.4(22)T	This command was modified. The **sip-request-pstn**keyword was added.
IOS Release XE 2.5	This command was integrated into Cisco IOS XE Release 2.5.

Examples

The following is sample output from the **show sip-ua map pstn-sip**command:

```
Router# show sip-ua map pstn-sip
PSTN-Cause   Configured        Default
             SIP-Status       SIP-Status
1               404             404
2               404             404
3               404             404
4               500             500
5               500             500
6               500             500
7               500             500
8               500             500
9               500             500
.
.
.
100             500             500
101             500             500
102             408             408
103             500             500
110             500             500
```

```
111             400             400
126             500             500
127             500             500
```

The following is sample output from the **show sip-ua map sip-pstn**command:

```
Router# show sip-ua map sip-pstn
SIP-Status   Configured        Default
             PSTN-Cause      PSTN-Cause
400             127             127
401             57              57
402             21              21
403             57              57
404             1               1
405             127             127
406             127             127
407             21              21
408             102             102
409             41              41
410             1               1
.
.
.
600             17              17
603             21              21
604             1               1
606             58              58
```

```
The following is sample output from the show sip
-ua map request
-pstn
command:
Router# show sip-request-pstn
SIP-Status   Configured        Default
             PSTN-Cause      PSTN-Cause
CANCEL          16              16
```

The table below describes the significant fields shown in the displays.

Table 140: show sip-ua map Field Descriptions

Field	Description
PSTN-Cause	Reasons for PSTN call failure or completion. PSTN cause code range is from 1 to 127.
Configured SIP-Status	Configured SIP status code or event. SIP Status code range is from 400 to 699.
Default SIP-Status	Default mapping between and PSTN and SIP networks.
SIP-Status	Configured SIP status code or event. SIP status code range is from 400 to 699.
Configured PSTN-Cause	Reasons for PSTN call failure or completion. PSTN cause code range is from 1 to 127.
Default PSTN-Cause	Default mapping between and SIP and PSTN networks.

Related Commands

Command	Description
set pstn-cause	Sets an incoming PSTN release cause code to a SIP error status code.
set sip-status	Sets an incoming SIP error status code to a PSTN release cause code.
sip-ua	Enables the SIP user-agent configuration commands.

show sip-ua min-se

To show the current value of the minimum session expiration (Min-SE) header for calls that use the Session Initiation Protocol (SIP) session timer, use the **show sip-ua min-se** command in privileged EXEC mode.

show sip-ua min-se

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.2(11)T	This command was introduced.
12.4(9)T	The Min-SE header default time was changed from 3200 to 90 seconds.
IOS Release XE 2.5	This command was integrated into Cisco IOS XE Release 2.5.

Usage Guidelines

Use thiscommand to verify the value of the Min-SE header.

Examples

The following is sample output from thiscommand:

```
Router# show sip-ua min-se
SIP UA MIN-SE Value (seconds)
Min-SE: 90
```

The table below describes the fields shown in this output.

Table 141: show sip-ua min-se Field Descriptions

Field	Description
SIP UA MIN-SE Value (seconds)	Field header indicating that the following information shows the current value of the Min-SE header, in seconds.
Min-SE	Current value of the Min-SE header, in seconds.

Related Commands

Command	Description
min-se (SIP)	Changes the Min-SE header value for all calls that use the SIP session timer.

show sip-ua mwi

To display Session Initiation Protocol (SIP) message-waiting indication (MWI) settings on the voice-mail server, use the **show sip-ua mwi command in**privileged EXEC mode.

show sip-ua mwi

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.3(8)T	This command was introduced.

Examples

The following is sample output from the **show sip-ua mwi**command:

```
Router#
show sip-ua mwi
MWI type: 2
MWI server: dns:unity-vm.gb.com
MWI expires: 60
MWI port: 5060
MWI transport type: UDP
MWI unsolicited
MWI server IP address:
C801011E
0
0
0
0
0
0
0
MWI ipaddr cnt 1:
MWI ipaddr idx 0:
MWI server: 192.168.1.30, port 5060, transport 1
MWI server dns lookup retry cnt: 0
endpoint 8000  mwi status ON
endpoint 8000  mwi status ON
endpoint 8001  mwi status OFF
```

The table below provides a listing of the fields in the sample output.

Table 142: show sip-ua mwi Field Descriptions

Field	Description
MWI type	Indicates the type of MWI service. 1 indicates MWI application service, which is used when a router provides MWI relay service. 2 indicates SIP-based MWI.

Field	Description
MWI server	Indicates the host device housing the domain name server (DNS) that resolves the name of the voice-mail server.
MWI expires	Indicates the expiration time, in seconds.
MWI port	Indicates the port used by SIP signaling.
MWI transport type	Indicates the desired transport protocol. Values are tcp or udp. UDP is the default.
MWI unsolicited	Indicates whether unsolicited MWI is configured.
MWI server IP address	Indicates the IP address of the voice-mail MWI server in hex format. If you configured the **mwi-server** command for DNS format, DNS lookup may result in multiple IP addresses. All IP addresses are listed.
MWI ipaddr cnt	Indicates the number of IP addresses associated with the voice-mail MWI server.
MWI ipaddr idx	Indicates which MWI server IP address is currently being used. The index starts from 0.
MWI server	Indicates the IP address of the MWI server; the port; and transport protocol (1 indicates UDP; 2 indicates TCP).
MWI server dns lookup retry cnt	Indicates the number of retries for DNS lookup.
endpoint / mwi status	Indicates the endpoint or voice port and whether MWI notification is active. That is, if a message is waiting, the status is on. Once the message is deleted, the status is off.

Related Commands

Command	Description
show sip-ua retry	Displays SIP retry statistics.
show sip-ua statistics	Displays response, traffic, and retry SIP statistics.
show sip-ua timers	Displays the current settings for SIP UA timers.
sip-ua	Enables the SIP user-agent configuration commands.

show sip-ua register status

To display the status of E.164 numbers that a Session Initiation Protocol (SIP) gateway has registered with an external primary SIP registrar, use the **show sip-ua register status**command in privileged EXEC mode.

show sip-ua register status [**secondary**]

Syntax Description

secondary	(Optional) Displays the status of E.164 numbers that a SIP gateway has registered with an external secondary SIP registrar.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.2(15)ZJ	This command was introduced.
12.3(4)T	This command was integrated into Cisco IOS Release 12.3(4)T.

Usage Guidelines

SIP gateways can register E.164 numbers on behalf of analog telephone voice ports (FXS), IP phone virtual voice ports (EFXS), and SCCP phones with an external SIP proxy or SIP registrar. The command **show sip-ua register status**is only for outbound registration, so if there are no SCCP phones or FXS dialpeers to register, there is no output when the command is run.

Examples

The following is sample output from this command:

```
Router# show sip-ua register status
Line peer expires(sec) registered
4001 20001 596         no
4002 20002 596         no
5100 1     596         no
9998 2     596         no
```

The table below describes significant fields shown in this output.

Table 143: show sip-ua register status Field Descriptions

Field	Description
Line	The phone number to register.
peer	The registration destination number.
expires (sec)	The amount of time, in seconds, until registration expires.
registered	Registration status.

Related Commands

Command	Description
registrar	Enables SIP gateways to register E.164 numbers on behalf of analog telephone voice ports (FXS), IP phone virtual voice ports (EFXS), and SCCP phones with an external SIP proxy or SIP registrar.

show sip-ua retry

To display retry statistics for the Session Initiation Protocol (SIP) user agent (UA), use the show sip-ua retrycommand in privileged EXEC mode.

show sip-ua retry

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.1(3)T	This command was introduced.
12.2(2)XB	Command output was enhanced to display the following: Reliable provisional responses (PRACK/reliable 1*xx*), Conditions met (COMET) responses, and Notify responses.
12.2(2)XB1	This command was implemented on the Cisco AS5850.
12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T. Support for the Cisco AS5300, Cisco AS5350, and Cisco AS5400 is not included in this release. For the purposes of display, this command was separated from the generic **show sip-ua**command found previously in this reference.
12.2(11)T	This command is supported on the Cisco AS5300, Cisco AS5350, and the Cisco AS5400 in this release.
12.2(15)T	This command is supported on the Cisco 1700 series, Cisco 2600 series, Cisco 3600 series, and the Cisco 7200 series routers in this release.

Usage Guidelines

Use this command to verify SIP configurations.

Examples

The following is sample output from this command.

```
Router# show sip-ua retry
SIP UA Retry Values
invite retry count = 6 response retry count = 1
bye retry count = 1 cancel retry count = 1
prack retry count = 10 comet retry count = 10
reliable 1xx count = 6 notify retry count = 10
```

The table below describes significant fields shown in this output, in alphabetical order.

Table 144: show sip-ua retry Field Descriptions

Field	Description
bye retry count	Number of times that a Bye request is retransmitted.

Field	Description
cancel retry count	Number of times that a Cancel request is retransmitted.
comet retry count	Number of times that a COMET request is retransmitted.
invite retry count	Number of times that an Invite request is retransmitted.
notify retry count	Number of times that a Notify message is retransmitted.
prack retry count	Number of times that a PRACK request is retransmitted.
refer retry count	Number of times that a Refer request is retransmitted.
reliable 1*xx* count	Number of times that a Reliable 1*xx* request is retransmitted.
response retry count	Number of times that a Response request is retransmitted.
SIP UA Retry Values	Field header for SIP UA retry values.

Related Commands

Command	Description
retry comet	Configures the number of times that a COMET request is retransmitted.
retry prack	Configures the number of times the PRACK request is retransmitted.
retry rel1xx	Configures the number of times the reliable 1*xx* response is retransmitted.
show sip-ua statistics	Displays response, traffic, and retry SIP statistics.
show sip-ua status	Displays SIP UA status.
show sip-ua timers	Displays the current settings for SIP UA timers.
sip-ua	Enables the SIP user-agent configuration commands.

show sip-ua service

To display Session Initiation Protocol (SIP) user-agent (UA) service information, use the **show sip-ua service** command in privileged EXEC mode.

show sip-ua service

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.4(24)T	This command was introduced in a release earlier than Cisco IOS Release 12.4(24)T.

Examples

The following example displays output when SIP UA call service is enabled:

```
Router# show sip-ua service

SIP Service is up
```

The following example displays output when SIP call service is shut down with the **shutdown** command:

```
Router# show sip-ua service
SIP service is shut globally
under 'voice service voip'
```

The following example displays output when SIP call service is shut down with the **call service stop** command:

```
Router# show sip-ua service
SIP service is shut
under 'voice service voip', 'sip' submode
```

The following example displays output when SIP call service is stopped forcefully with the **call service stop forced** command:

```
Router# show sip-ua service
SIP service is forced shut
under 'voice service voip', 'sip' submode
```

The following example displays output when SIP call service is forcefully shutdown globally with the **shutdown forced** command:

```
Router# show sip-ua service
SIP service is forced shut globally
under 'voice service voip'
```

The fields in the displays are self-explanatory.

Related Commands

Command	Description
call service stop	Shuts down VoIP call service on a gateway.
voice service	Enters voice-service configuration mode and specifies a voice-encapsulation type.

show sip-ua srtp

To display Session Initiation Protocol (SIP) user-agent (UA) Secure Real-time Transport Protocol (SRTP) information, use the **show sip-ua srtp** command in privileged EXEC mode.

show sip-ua srtp

Syntax Description

This command has no keywords or arguments.

Command Default

SIP UA SRTP information is not displayed.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS 15.4(1)T	This command was introduced.
Cisco IOS XE Everest 16.5.1b	Command output was updated to show AEAD_AES_256_GCM and AEAD_AES_128_GCM cipher suites.

Example

The following example displays sample output for SIP UA SRTP information prior to Cisco IOS XE Everest Release 16.5.1b:

```
Device> enable
Device# show sip-ua srtp
SIP UA SRTP
Crypto-suite Negotiation
  AES_CM_128_HMAC_SHA1_80: 3
  AES_CM_128_HMAC_SHA1_32: 2
```

The following example displays the sample output for SIP UA SRTP information including AEAD_AES_256_GCM and AEAD_AES_128_GCM cipher suites supported from Cisco IOS XE Everest Release 16.5.1b:

```
Device> enable
Device# show sip-ua srtp
SIP UA SRTP
Crypto-suite Negotiation
  AES_CM_128_HMAC_SHA1_80: 3
  AES_CM_128_HMAC_SHA1_32: 2
  AEAD_AES_256_GCM: 1
  AEAD_AES_128_GCM: 2
```

Related Commands

Command	Description
voice class srtp-crypto	From Cisco IOS XE Everest 16.5.1b onwards, this command is used to configure a Secure Real-time Transport Protocol (SRTP) connection on Cisco Unified Border Element (CUBE) in the global level using the preferred crypto suite.

Command	Description
srtp-auth	Configures a Secure Real-time Transport Protocol (SRTP) connection on Cisco Unified Border Element (CUBE) in the global level using the preferred crypto suite.
voice-class sip srtp-auth	Configures a Secure Real-time Transport Protocol (SRTP) connection on Cisco Unified Border Element (CUBE) in the dial peer level using the preferred crypto suite.

show sip-ua statistics

To display response, traffic, and retry Session Initiation Protocol (SIP) statistics, use the **show sip-ua statistics** command in privileged EXEC mode.

show sip-ua statistics [**dial-peer**] *tag*

Syntax Description

tag	A unique number (for example, 1, 100, etc.) identifying the dial peer. Value range: 1-2147483647
dial-peer	Displays SIP UA dial-peer statistics.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE 17.18.2	The command is modified to display the SIP global error counters for the dial-peer.
Cisco IOS Release XE 3.12S	Command output was enhanced to display the SIP error counters: • Number of times a particular error has occurred. • The error string for immediate context • Timestamp of first occurrence • Timestamp of last occurrence
15.4(2)T	Command output was enhanced to display the SIP error counters: • Number of times a particular error has occurred. • The error string for immediate context • Timestamp of first occurrence • Timestamp of last occurrence
IOS Release XE 2.5	This command was integrated into Cisco IOS XE Release 2.5.
12.3(4)T	This command was integrated into Cisco IOS Release 12.3(4)T. Command output was enhanced to display SUBSCRIBE retry statistics.
12.2(15)ZJ	Command output was enhanced to display the following: • Register counter and statistics.
12.2(15)T	This command is supported on the Cisco 1700 series, Cisco 2600 series, Cisco 3600 series, and the Cisco 7200 series routers in this release.

Release	Modification
12.2(13)T	This command was supported in Cisco IOS Release 12.2(13)T. The following cause codes were obsoleted from the command output: • Redirection code: *SeeOther* • Client Error: *LengthRequired* A new SIP statistics counter was added: • Miscellaneous Counters: *RedirectResponseMappedToClientError* Command output was enhanced to display the following: • Time stamp that indicates the last time that SIP statistics counters were cleared.
12.2(11)T	This command was integrated into Cisco IOS Release 12.2(11)T. Command output was enhanced as follows: • OkInfo counter (200) class counts the number of successful responses to INFO requests. • Info counter counts the number of INFO messages received and sent. • BadEvent counter (489 response) counts responses to Subscribe messages with event types that are not understood by the server. • OkSubscribe counter (200 class) counts the number of 200 OK SIP messages received and sent in response to Subscribe messages. • Subscribe requests indicate total requests received and sent. • SDP application statistics added to monitor SDP. This command was supported on the Cisco AS5300, Cisco AS5350, and Cisco AS5400 in this release.
12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T. Support for the Cisco AS5300, Cisco AS5350, and Cisco AS5400 was not included in this release. For the purposes of display, this command was separated from the generic **show sip-ua** command.
12.2(2)XB1	This command was implemented on the Cisco AS5850.
12.2(2)XB	Command output was enhanced as follows: BadRequest counter (400 class) now counts malformed Via entries, reliable provisional responses (PRACK/rel1*xx*), conditions met (COMET), and NOTIFY responses.
12.2(2)XA	This command was implemented on the Cisco AS5350 and Cisco AS5400.
12.1(3)T	This command was introduced.

Usage Guidelines

Use the **show sip-ua statistics** command to verify SIP configurations and to see SIP global counters. You can also use this command to see the number of times a particular error has occurred. This command is typically

helpful when enabling CCSIP error debugs is not desirable. Along with other data, the error counters will provide better code-flow context, so that the issue can be reproduced and targeted RCA can be performed.

Examples

The following is a sample output displaying the SIP global error counters for the dial-peer 16:

```
Router# show sip-ua statistics dial-peer 16
SIP Counters:
  <File Id, Line:  Count    First Occurence         Most Recent Occurence     Message>
    0x21  , 2973  : 1       Sep 17 2025 14:25:24    Sep 17 2025 14:25:24      Invalid
deferredQueue
    0x41  , 884   : 1       Sep 17 2025 14:25:23    Sep 17 2025 14:25:23      main stream,
 No DNS involved
    0x41  , 888   : 1       Sep 17 2025 14:25:23    Sep 17 2025 14:25:23      not a main
stream, use loopback address
    0x41  , 980   : 1       Sep 17 2025 14:25:23    Sep 17 2025 14:25:23
resolve_sig_ip_address_to_bind failed
    0x41  , 21402 : 1       Sep 17 2025 14:25:23    Sep 17 2025 14:25:23      Failed to get
 source addres for IPv4 stream
    0x6A  , 2134  : 1       Sep 17 2025 14:25:24    Sep 17 2025 14:25:24      ws_info is
NULL
```

The following is a sample output from this command:

```
Router# show sip-ua statistics
SIP Response Statistics (Inbound/Outbound)
    Informational:
      Trying 0/0, Ringing 0/0,
      Forwarded 0/0, Queued 0/0,
      SessionProgress 0/0
     Success:
      OkInvite 0/0, OkBye 0/0,
      OkCancel 0/0, OkOptions 0/0,
      OkPrack 0/0, OkPreconditionMet 0/0,
      OkSubscribe 0/0, OkNOTIFY 0/0,
      OkInfo 0/0, 202Accepted 0/0
      OkRegister 12/49
     Redirection (Inbound only except for MovedTemp(Inbound/Outbound)) :
      MultipleChoice 0, MovedPermanently 0,
      MovedTemporarily 0/0, UseProxy 0,
      AlternateService 0
      Client Error:
      BadRequest 0/0, Unauthorized 0/0,
      PaymentRequired 0/0, Forbidden 0/0,
      NotFound 0/0, MethodNotAllowed 0/0,
      NotAcceptable 0/0, ProxyAuthReqd 0/0,
      ReqTimeout 0/0, Conflict 0/0, Gone 0/0,
      ReqEntityTooLarge 0/0, ReqURITooLarge 0/0,
      UnsupportedMediaType 0/0, BadExtension 0/0,
      TempNotAvailable 0/0, CallLegNonExistent 0/0,
      LoopDetected 0/0, TooManyHops 0/0,
      AddrIncomplete 0/0, Ambiguous 0/0,
      BusyHere 0/0, RequestCancel 0/0,
      NotAcceptableMedia 0/0, BadEvent 0/0,
      SETooSmall 0/0
     Server Error:
      InternalError 0/0, NotImplemented 0/0,
      BadGateway 0/0, ServiceUnavail 0/0,
      GatewayTimeout 0/0, BadSipVer 0/0,
      PreCondFailure 0/0
     Global Failure:
```

```
      BusyEverywhere 0/0, Decline 0/0,
      NotExistAnywhere 0/0, NotAcceptable 0/0
      Miscellaneous counters:
      RedirectRspMappedToClientErr 0
SIP Total Traffic Statistics (Inbound/Outbound)
      Invite 0/0, Ack 0/0, Bye 0/0,
      Cancel 0/0, Options 0/0,
      Prack 0/0, Comet 0/0,
      Subscribe 0/0, NOTIFY 0/0,
      Refer 0/0, Info 0/0
      Register 49/16
Retry Statistics
      Invite 0, Bye 0, Cancel 0, Response 0,
      Prack 0, Comet 0, Reliable1xx 0, Notify 0
      Register 4, Subscribe 0
SDP application statistics:
Parses: 0, Builds 0
Invalid token order: 0, Invalid param: 0
Not SDP desc: 0, No resource: 0
Last time SIP Statistics were cleared: <never>
```

Command output, listed in **Table 1** includes a reason phrase and a count describing the SIP messages received and sent. When x/x is included in the reason phrase field, the first number is an inbound count, and the second number is an outbound count. The description field headings are based on the SIP response code xxx, which the SIP protocol uses in determining behavior. SIP response codes are classified into one of the following six categories:

- 1xx: Informational, indicates call progress.
- 2xx: Success, indicates successful receipt or completion of a request.
- 3xx: Redirection, indicates that a redirect server has returned possible locations.
- 4xx: Client error, indicates that a request cannot be fulfilled as it was submitted.
- 5xx: Server error, indicates that a request has failed because of an error by the server. The request may be retried at another server.
- 6xx: Global failure, indicates that a request has failed and should not be tried again at any server.

The table below describes significant fields shown in this output, in alphabetical order.

Table 145: show sip-ua statistics Field Descriptions

Field	Description
Note For each field, the standard RFC 2543 SIP response number and message are shown.	
Ack 0/0	A confirmed final response received or sent.
Accepted 0/0	202 A successful response to a Refer request received or sent.
AddrIncomplete 0/0	484 Address supplied is incomplete.
AlternateService 0	380 Unsuccessful call; however, an alternate service is available.

Field	Description
Ambiguous 0/0	485 Address supplied is ambiguous.
BadEvent 0/0	489 Bad Event response indicates a Subscribe request having an event type that the server could not understand.
BadExtension 0/0	420 Server could not understand the protocol extension in the Require header.
BadGateway 0/0	502 Network is out of order.
BadRequest	400 Bad Request (includes the malformed Via header).
BadSipVer 0/0	505 Requested SIP version is not supported.
BusyEverywhere 0/0	600 Called party is busy.
BusyHere 0/0	486 Called party is busy.
Bye 0	Number of times that a Bye request is retransmitted to the other user agent.
Bye 0/0	Terminated the session.
CallLegNonExistent 0/0	481 Server is ignoring the request. Either is was a Bye request and there was no matching leg ID, or it was a Cancel request and there was no matching transaction.
Cancel 0	Number of times that a Cancel request is retransmitted to the other user agent.
Cancel 0/0	Terminated the pending request.
Comet 0	Number of times that a COMET request is retransmitted to the other user agent.
Comet 0/0	Conditions have been met.
Conflict 0/0	409 Temporary failure.
Decline 0/0	603 Call rejected.
Forbidden 0/0	403 The SIP server has the request, but cannot provide service.
Forwarded 0/0	181 Call has been forwarded.
GatewayTimeout 0/0	504 The server or gateway did not receive a timely response from another server (such as a location server).
Gone 0/0	410 Resource is no longer available at the server, and no forwarding address is known.

Field	Description
Info 0/0	Number of information messages the gateway has received (inbound) and how many have been transmitted (outbound).
InternalError 0/0	500 The server or gateway encountered an unexpected error that prevented it from processing the request.
Invite 0	Number of times that an INVITE request is retransmitted to the other user agent.
Invite 0/0	Initiates a call.
LoopDetected 0/0	482 A loop--server received a request that included itself in the path.
MethodNotAllowed 0/0	405 Method specified in the request is not allowed.
MovedPermanently 0	301 User is no longer available at this location.
MovedTemporarily 0	302 User is temporarily unavailable.
MultipleChoice 0	300 Address resolves to more than one location.
NotAcceptable 0/0	406/606 Call was contacted, but some aspect of the session description was unacceptable.
NotAcceptableMedia 0/0	406 Call was contacted, but some aspect of the session description was unacceptable.
NotExistAnywhere 0/0	604 Server has authoritative information that the called party does not exist in the network.
NotFound 0/0	404 Called party does not exist in the specified domain.
NOTIFY 0	Number of times that a Notify is retransmitted to the other user agent.
NOTIFY 0/0	Number of Notify messages received or sent.
NotImplemented 0/0	501 Service or option not implemented in the server or gateway.
OkBye 0/0	200 Successful response to a Bye request.
OkCancel 0/0	200 Successful response to a Cancel request.
OkInfo	200 Successful response to an INFO request.
OkInvite 0/0	200 Successful response to an INVITE request.
OkNOTIFY 0/0	200 Successful response to a Notify request.
OkOptions 0/0	200 Successful response to an Options request.

Field	Description
OkPrack 0/0	200 Successful response to a PRACK request.
OkPreconditionMet 0/0	200 Successful response to a PreconditionMet request.
OkRegister 0/0	200 Successful response to a Register request.
OkSubscribe 0/0	200 Successful response to a SUBSCRIBE request.
Options 0/0	Query the receiving or sending server as to its capabilities.
PaymentRequired 0/0	402 Payment is required to complete the call.
Prack 0	Number of times that a PRACK request is retransmitted to the other user agent.
Prack 0/0	Provisional response received or sent.
PreCondFailure 0/0	580 The session could not be established because of failure to meet required preconditions.
ProxyAuthReqd 0/0	407 Rejected for proxy authentication.
Queued 0/0	182 Until the called party is available, the message is queued.
RedirectResponseMappedToClientError 0	Indicates the count of incoming 3*xx* responses that were mapped to 4*xx* responses. It is incremented when the **no redirection** command is active. For the default case, the 3*xx* messages are processed per RFC 2543, and this counter is not incremented. This counter counts only inbound messages and only the 3*xx* responses that are known (300, 301, 302, 305, and 380). The counter is cleared when the **clear sip-ua statistics** command is issued.
Refer 0	Number of times the Refer request is retransmitted to the other user agent.
Refer 0/0	Number of Refer requests received or sent.
Register 0/0	Number of Register requests received or sent.
Register 0	Number of times that a Register request is retransmitted to the other user agent.
Reliable1xx 0	Indicates the number of times the Reliable 1*xx* response is retransmitted to the other user agent.
ReqEntityTooLarge 0/0	413 Server refuses to process request because the request is larger than is acceptable.

Field	Description
ReqTimeout 0/0	408 Server could not produce a response before the Expires time- out.
RequestCancel 0/0	Request has been canceled.
ReqURITooLarge 0/0	414 Server refuses to process, because the URI (URL) request is larger than is acceptable.
Response 0	Indicates number of Response retries.
Retry Statistics	One of the three categories of response statistics.
Ringing 0/0	180 Called party has been located and is being notified of the call.
SeeOther 0	303 Transfer to another address.
ServiceUnavail 0/0	503 Service option is not available because of an overload or maintenance problem.
SessionProgress 0/0	183 Indicates in-band alerting.
SIP Response Statistics (Inbound/Outbound)	One of the three categories of response statistics.
SIP Total Traffic Statistics (Inbound/Outbound)	One of the three categories of response statistics.
Subscribe 0	Indicates the number of Retry Subscribe messages sent.
Subscribe 0/0	Number of Subscribe requests received or sent.
TempNotAvailable 0/0	480 Called party did not respond.
TooManyHops 0/0	483 A server received a request that required more hops than is allowed by the Max-Forward header.
Trying 0/0	100 Action is being taken with no resolution.
Unauthorized 0/0	401 The request requires user authentication.
UnsupportedMediaType 0/0	415 Server refuses to process a request because the service option is not available on the destination endpoint.
UseProxy 0	305 Caller must use a proxy to contact called party.

Examples

The following is a sample output from this command that displays the SIP global counters—the error string for immediate context, timestamp for first occurrence of error, and timestamp for last occurrence of error:

```
Device# show sip-ua statistics | sec SIP Global Counters

<File Id, Line: Count  First     Most Recent
    Message>
```

```
0x41, 664   :     2      Nov 08 2013 11:41:56 Nov 08 2013 11:46:14
  main stream, No DNS involved
0x41, 760   :     2      Nov 08 2013 11:41:56 Nov 08 2013 11:46:14
  resolve_sig_ip_address_to_bind failed
0x41, 7293  :     10     Nov 08 2013 11:41:56 Nov 08 2013 11:46:14
  Unexpected VoIPCodec Type :%s
0x41, 10147 :     2      Nov 08 2013 11:41:56 Nov 08 2013 11:46:14
  Offered ptime:%d, Negotiated ptime:%d Negotiated codec bytes: %d for codec %s
0x41, 10941 :     2      Nov 08 2013 11:41:56 Nov 08 2013 11:46:14
  No voice codec and no dtmf-relay match
0x41, 13012 :     2      Nov 08 2013 11:41:56 Nov 08 2013 11:46:14
  Media negotiation failed for m-line %d
```

Related Commands

Command	Description
show sip-ua retry	Displays SIP retry statistics.
show sip-ua status	Displays SIP UA status.
show sip-ua timers	Displays the current settings for SIP UA timers.
sip-ua	Enables the SIP user-agent configuration commands.

show sip-ua status

To display status for the Session Initiation Protocol (SIP) user agent (UA), use the **show sip-ua status**command in privileged EXEC mode.

show sip-ua status

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.1(1)T	This command was introduced on the Cisco 2600 series, Cisco 3600 series, and Cisco AS5300.
12.1(3)T	The statistics portion of the output was removed and included in the **show sip-ua statistics** command.
12.2(2)XA	This command was implemented on the Cisco AS5350 and Cisco AS5400.
12.2(2)XB	Command output was enhanced to display if media or signaling binding is enabled, and the style of the DNS SRV query (1 for RFC 2052; 2 for RFC 2782).
12.2(2)XB1	This command was implemented on the Cisco AS5850.
12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T. Support for the Cisco AS5300, Cisco AS5350, and Cisco AS5400 was not included in this release. For the purposes of display, this command was separated from the generic **show sip-ua** command.
12.2(11)T	Command output was enhanced to display information on Session Description Protocol (SDP) application configuration. This command was supported on the Cisco AS5300, Cisco AS5350, Cisco AS5400, and Cisco AS5850 in this release.
12.2(13)T	Command output was enhanced to display the following: Information on redirection message handling. Information on handling of 180 responses with SDP.
12.2(15)T	Command output was enhanced to display Suspend and Resume support.
12.2(15)ZJ	Command output was enhanced to display information on the duration of dual-tone multifrequency (DTMF) events.
12.3(4)T	This command was integrated into Cisco IOS Release 12.3(4)T.
12.3(8)T	Command output was enhanced to display Reason Header support.
12.4(22)T	Command output was updated to show IPv6 information.

Release	Modification
Cisco IOS Release XE 2.5	This command was integrated into Cisco IOS XE Release 2.5.

Usage Guidelines

Use this command to verify SIP configurations.

Examples

The following is sample output from the **show sip-ua status** command:

```
Router# show sip-ua status
SIP User Agent Status
SIP User Agent for UDP : ENABLED
SIP User Agent for TCP : ENABLED
SIP User Agent for TLS over TCP : ENABLED
SIP User Agent bind status(signaling): DISABLED
SIP User Agent bind status(media): DISABLED
SIP early-media for 180 responses with SDP: ENABLED
SIP max-forwards : 70
SIP DNS SRV version: 2 (rfc 2782)
NAT Settings for the SIP-UA
Role in SDP: NONE
Check media source packets: DISABLED
Maximum duration for a telephone-event in NOTIFYs: 2000 ms
SIP support for ISDN SUSPEND/RESUME: ENABLED
Redirection (3xx) message handling: ENABLED
Reason Header will override Response/Request Codes: DISABLED
Out-of-dialog Refer: DISABLED
Presence support is DISABLED
protocol mode is ipv4
SDP application configuration:
 Version line (v=) required
 Owner line (o=) required
 Timespec line (t=) required
 Media supported: audio video image
 Network types supported: IN
 Address types supported: IP4 IP6
 Transport types supported: RTP/AVP udptl
```

The following is sample output from the **show sip-ua status** command showing IPv6 information:

```
Router# show sip-ua status
SIP User Agent Status
SIP User Agent for UDP : ENABLED
SIP User Agent for TCP : ENABLED
SIP User Agent for TLS over TCP : ENABLED
SIP User Agent bind status(signaling): DISABLED
SIP User Agent bind status(media): DISABLED
SIP early-media for 180 responses with SDP: ENABLED
SIP max-forwards : 70
SIP DNS SRV version: 2 (rfc 2782)
NAT Settings for the SIP-UA
Role in SDP: NONE
Check media source packets: DISABLED
Maximum duration for a telephone-event in NOTIFYs: 2000 ms
SIP support for ISDN SUSPEND/RESUME: ENABLED
Redirection (3xx) message handling: ENABLED
Reason Header will override Response/Request Codes: DISABLED
Out-of-dialog Refer: DISABLED
Presence support is DISABLED
protocol mode is ipv6
SDP application configuration:
```

```
 Version line (v=) required
Owner line (o=) required
 Timespec line (t=) required
 Media supported: audio video image
 Network types supported: IN
 Address types supported: IP4 IP6
 Transport types supported: RTP/AVP udptl
```

The table below describes the significant fields shown in the display.

Table 146: show sip-ua status Field Descriptions

Field	Description
SIP User Agent Status	UA status.
SIP User Agent for UDP	User Datagram Protocol (UDP) is enabled or disabled.
SIP User Agent for TCP	TCP is enabled or disabled.
SIP User Agent bind status (signaling)	Binding for signaling is enabled or disabled.
SIP User Agent bind status (media)	Binding for media is enabled or disabled.
SIP early-media for 180 responses with SDP	Early media cut-through treatment for 180 responses with SDP can be enabled (the default treatment) or disabled, with local ringback provided.
SIP max-forwards	Value of max-forwards of SIP messages.
SIP DNS SRV version	Style of the DNS SRV query: 1 for RFC 2052 or 2 for RFC 2782.
NAT Settings for the SIP-UA	Symmetric Network Address Translation (NAT) settings when the feature is enabled.
Role in SDP	Identifies the endpoint function in the connection setup procedure during symmetric NAT traversal. The endpoint role may be set to active, meaning that it initiates a connection, or to passive, meaning that it accepts a connection. A value of none in this field means that the feature is disabled.
Check media source packets	Media source packet checking is enabled or disabled.
Maximum duration for a telephone-event in NOTIFYs	Shows the time interval, in milliseconds (ms), between consecutive NOTIFY messages for a telephone event.
SIP support for ISDN SUSPEND/RESUME	Suspend and Resume support is enabled or disabled.
Redirection (3xx) message handling	Redirection can be enabled, which is the default status, according to RFC 2543. Or handling of redirection 3*xx* messages can be disabled, allowing the gateway to treat 3*xx* redirect messages as 4*xx* error messages.
Reason Header will override Response/Request Codes	Reason header is enabled or disabled.

Field	Description
protocol mode is ipv6	States whether the protocol being used is IPv6 or IPv4.
Version line (v=)	Indicates if the SDP version is required.
Owner line (o=)	Indicates if the session originator is required.
Timespec line (t=)	Indicates if the session start and stop times are required.
Media supported	Media information.
Network types supported	Always IN for Internet.
Address types supported	Identifies the Internet Protocol version.
Transport types supported	Identifies the transport protocols supported.

Related Commands

Command	Description
show sip -ua retry	Displays SIP retry statistics.
show sip -ua statistics	Displays response, traffic, and retry SIP statistics.
show sip -ua timers	Displays the current settings for SIP UA timers.
sip -ua	Enables the SIP user-agent configuration commands.

show sip-ua status refer-ood

To display the number of incoming and outgoing out-of-dialog REFER (OOD-R) connections, use the **show sip-ua status refer-ood** command in privileged EXEC mode.

show sip-ua status refer-ood

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.4(11)XJ	This command was introduced.
12.4(15)T	This command was integrated into Cisco IOS Release 12.4(15)T.

Usage Guidelines

Use this command to verify OOD-R processing.

Examples

The following is sample output from the **show sip-ua status refer-ood** command:

```
Router# show sip-ua status refer-ood
Maximum allow incoming out-of-dialog refer 500
Current existing incoming out-of-dialog refer dialogs: 1
                 outgoing out-of-dialog refer dialogs: 0
```

The table below describes significant fields shown in this output.

Table 147: show sip-ua status refer-ood Field Descriptions

Field	Description
Maximum allow incoming out-of-dialog refer	Maximum number of incoming OOD-R sessions that the router is allowed. Value set by the **refer-ood enable** command. Default is 500.
Current existing incoming out-of-dialog refer dialogs	Number of currently active incoming OOD-R sessions.
outgoing out-of-dialog refer dialogs	Number of currently active outgoing OOD-R sessions used for line status updates.

Related Commands

Command	Description
refer-ood enable	Enables OOD-R processing.
show sip -ua retry	Displays SIP retry statistics.
show sip -ua statistics	Displays response, traffic, and retry SIP statistics.

Command	Description
sip -ua	Enables the SIP user-agent configuration commands.

show sip-ua timers

To display the current settings for the Session Initiation Protocol (SIP) user-agent (UA) timers, use the **show sip-ua timers** command in privileged EXEC mode.

show sip-ua timers

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.1(1)T	This command was introduced on the Cisco 2600 series, Cisco 3600 series, and Cisco AS5300.
12.1(3)T	The output of this command was changed to reflect the various forms of the timers command.
12.2(2)XA	This command was implemented on the Cisco AS5350 and Cisco AS5400.
12.2(2)XB	Command output was enhanced to display the following: Reliable provisional responses (PRACK/rel 1*xx*), Conditions met (COMET), and NOTIFY responses.
12.2(2)XB1	This command was implemented on the Cisco AS5850.
12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T. Support for the Cisco AS5300, Cisco AS5350, and Cisco AS5400 was not included in this release. For the purposes of display, this command was separated from the generic **show sip-ua**command found previously in this reference.
12.2(11)T	This command was supported on the Cisco AS5300, Cisco AS5350, Cisco AS5400, and Cisco AS5850 in this release.
12.2(11)YT	Command output was enhanced to display Refer responses.
12.2(15)T	This command was supported on the Cisco 1700 series, Cisco 2600 series, Cisco 3600 series, and the Cisco 7200 series routers in this release.
12.3(1)	Command output was enhanced to display the SIP hold timer value.
12.2(15)ZJ	Command output was enhanced to display Register responses.
12.3(4)T	This command was integrated into Cisco IOS Release 12.3(4)T.
12.3(8)T	Command output was enhanced to display the buffer-invite timer value and the connection aging timer value.
Cisco IOS XE Bengaluru 17.4.1a	Command output was enhanced to display the time to wait before establishing a TLS connection with the remote server.

Usage Guidelines

Use this command to verify SIP configurations.

Examples

The following is sample output from this command:

```
Router# show sip-ua timers
SIP UA Timer Values (millisecs unless noted)
trying 500, expires 180000, connect 500, disconnect 500
prack 500, rel1xx 500, notify 500, update 500
refer 500, register 500, info 500, options 500,hold 2880 minutes
, register-dns-cache 3600 seconds
tcp/udp aging 5 minutes
tls aging 60 minutes
tls establish 20 seconds
```

The table below describes significant fields shown in this output.

Table 148: show sip-ua timers Field Descriptions

Field	Description
SIP UA Timer Values (millisecs)	SIP UA timer status.
trying	Time to wait before a Trying message is retransmitted.
expires	Time to wait before an Expires message is retransmitted.
connect	Time to wait before a Connect message is retransmitted.
disconnect	Time to wait before a Disconnect message is retransmitted.
prack	Time to wait before a PRACK acknowledgment is retransmitted.
rel1xx	Time to wait before a Rel1*xx* response is retransmitted.
notify	Time to wait before a Notify response is retransmitted.
refer	Time to wait before a Retry request is retransmitted.
register	Time to wait before a Register request is retransmitted.
hold	Time to wait in minutes before a BYE request is sent.
buffer-invite	Time to buffer the INVITE while waiting for display information.
tcp/udp aging	Time to wait in minutes before a TCP or UDP connection is aged out.
tls aging	Time to wait in minutes before a TLS connection is aged out.
tls establish	Time to wait in seconds for establishing a TLS connection with the remote server.

Related Commands

Command	Description
show sip-ua retry	Displays SIP retry statistics.

Command	Description
show sip-ua statistics	Displays response, traffic, and retry SIP statistics.
show sip-ua status	Displays SIP UA status.
sip-ua	Enables the SIP user-agent configuration commands.

show spe voice

To display voice-service-history statistics for a specified service processing element (SPE), use the **show spe voice** command in privileged EXEC mode.

show spe voice {[**active**] [*slot* | *slot*/*spe*] | **summary** [*slot* | *slot*/*spe*]}

Syntax Description

slot	All SPEs on the specified slot. Cisco AS5350 range: 1 to 3. Cisco AS5400 range: 1 to 7. Cisco AS5850 range: 0 to 13.
slot / *spe*	Specified SPE on the specified slot. Slot range: as above. SPE range as follows: • Cisco 5350 and Cisco 5400: 0 to 17 • Cisco 5850 (in a CT3_UP216 card): 0 to 35 • Cisco 5850 (in a UP324 card): 0 to 53 You must include the slash mark.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.2(2)XB	This command was introduced on the Cisco AS5350, Cisco AS5400, and Cisco AS5850.

Usage Guidelines

Use the *slot* or *slot*/*spe* argument once to specify a single slot or SPE. Use it twice to specify the first and last of a range of slots or SPEs.

The following examples specify the following: a single SPE, a single slot, a range of SPEs in a slot, and a range of slots:

```
show spe voice 1/3
show spe voice 1
show spe voice 1/1 1/3
show spe voice 1 3
```

The **summary** keyword permits you to employ output modifiers to the command so as to write large amounts of data output directly to a file for later reference. You can save this file on local or remote storage devices such as flash, a SAN disk, or an external memory device. You can write output to a new file or append it to an existing file and, optionally at the same time, display it onscreen. Redirection is available using a pipe (|) character combined with the **redirect**, **append**, or **tee** keywords.

For more information on output modifiers, see *Show Command Output Redirection* at the following location: http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t13/ftshowre.htm

Examples

The following example shows information for a single SPE (slot 2, SPE 1):

```
Router# show spe voice 2/1
#SPE 2/01
```

```
Cisco Universal SPE (Managed); Port 2/6 - 2/11
Last clearing of statistics counters          :  never
         0 Incoming calls                      0 Outgoing calls
   Voice:
         0 Payload Type Violation              0 Buffer Overflow Errors
         0 End-point Detection Errors          0 Packets Received Early
         0 Packets Received Late               0 Bad Protocol Headers
   Fax-relay:
         0 Payload Type Violation              0 Buffer Overflow Errors
         0 Buffer Underflow Errors             0 End-point Detection Errors
         0 Bad Protocol Headers
Codec          Calls   Codec     Calls   Codec           Calls   Codec     Calls
G.711 u-Law        0   G.729         0   G.723.1 6.3K        0   GSM FR        0
G.711 a-Law        0   G.729B        0   G.723.1 5.3K        0   GSM HR        0
G.726 40K          0   G.729A        0   G.723.1A 6.3K       0   GSM EFR       0
G.726 32K          0   G.729AB       0   G.723.1A 5.3K       0
G.726 24K          0   G.728         0   Clear Channel       0
G.726 16K          0
```

The following example shows summary information:

```
Router# show spe voice summary
Cisco Universal SPE (Managed); Port 1/0 - 1/107
Last clearing of statistics counters          :  never
         0 Incoming calls                      0 Outgoing calls
   Voice:
         0 Payload Type Violation              0 Buffer Overflow Errors
         0 End-point Detection Errors          0 Packets Received Early
         0 Packets Received Late               0 Bad Protocol Headers
   Fax-relay:
         0 Payload Type Violation              0 Buffer Overflow Errors
         0 Buffer Underflow Errors             0 End-point Detection
Errors
         0 Bad Protocol Headers
Codec          Calls   Codec     Calls   Codec           Calls   Codec       Calls
G.711 u-Law        0   G.729         0   G.723.1 6.3K        0   GSM FR      0
G.711 a-Law        0   G.729B        0   G.723.1 5.3K        0   GSM HR      0
G.726 40K          0   G.729A        0   G.723.1A 6.3K       0   GSM EFR     0
G.726 32K          0   G.729AB       0   G.723.1A 5.3K       0
G.726 24K          0   G.728         0   Clear Channel       0   G.726 16K   0
```

The table below describes the significant fields shown in the display.

Table 149: show spe voice Command Field Descriptions

Field	Description
SPE	Slot and port number of the SPE.
Last Clearing of Statistics Counters	Last time the statistics counters were cleared by means of the **clear spe counters** command.
Buffer Overflow Errors	The digital-signal-processor (DSP) buffer has overflowed. If overflow continues, data will be lost and voice will be distorted (as concealment is added).
Endpoint Detection Errors	A voice frame has arrived after a predefined timer expires, causing the DSP to declare it late. If the frame consists of the SID/marker bit, it causes an endpoint detection error and the late packet is included as an endpoint detection error.

Field	Description
Packets Received Early	The number of frames held in the delay buffer exceeds the expected playout delay -- that is, the delay buffer is overrun (too many frames waiting to be played out for the expected playout delay). At this point, the buffer must reduce the excess delay using intelligent frame deletion to preserve audio continuity.
Packets Received Late	The DSP has received an out-of-sequence packet and started a timer for the missing packet. The packet has failed to arrive in time; it is marked as late and the statistic is incremented. The DSP does interpolative or silence concealment for any missing frames. This type of problem is apt to occur in a congested network and results in lost packets and diminished voice quality.
Bad Protocol Headers	Packets have been rejected for any of the following reasons: bad protocol header, incorrect length, unknown packet format, unknown Real-Time Transport Protocol synchronization source (SSRC), incorrect checksum (when the Extended header is used), cumulative number of packets with invalid RTP headers (the header extension exceeds the packet length), or an invalid User Datagram Protocol (UDP)/IP header if extended encapsulation is enabled.

Related Commands

Command	Description
show spe	Displays SPE status.
show spe modem	Displays modem service-history statistics for a specified SPE.
show spe version	Displays the firmware version on a specified SPE.

show ss7 mtp1 channel-id

To display information for a given session channel ID, use the **show ss7 mtp1 channel-id** command in privileged EXEC mode.

show ss7 mtp1 channel-id [*channel*]

Syntax Description

channel	(Optional) Specific channel. Range is from 0 to 23.

Command Default

Information for all channels is displayed.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.2(11)T	This command was introduced.

Usage Guidelines

This command is useful for determining which channel IDs have already been allocated.

Examples

The following sample output displays the name of the serial interface for the link, the assigned media gateway controller (MGC) port, whether the link is serial (12-in-1 port) or digital (E1/T1 trunk DS0), the assigned channel ID, and whether the link is stopped or started:

```
Router# show ss7 mtp1 channel-id
  SS7 MTP1 Session-channel [all]:
       channel  assigned interface
       -------  ------------------
           0      7/0:0  (digital)
           1        7/0   (serial)
           3      7/0:1  (digital)
```

The table below describes significant fields shown in this output.

Table 150: show ss7 mtp1 channel-id Field Descriptions

Field	Description
SS7 MTP1 Session-channel	Information about channel IDs.
all	Information on all assigned channel IDs if a particular ID is not specified.
channel	Channel ID assigned by use of the channel-id command.
assigned	Name of the interface serial object to which the channel ID is assigned.
interface	Whether the link type is digital or serial.

The following sample output concerns a specified channel-ID parameter:

```
Router# show ss7 mtp1 channel-id 1

serial interface:  7/0:1 (digital)
  SCC port:          2
  link state:        STARTED
  IDB state:         IDBS_UP
  rcv-pool:
     pool-name:      Rcv07:02
     congested:      FALSE
     in-use buffers: 16
     free buffers:   384
  tx-pool:
     pool-name:      SS7txB01
     in-use buffers: 64
     free buffers:   1236
```

The table below describes significant fields shown in this output.

Table 151: show ss7 mtp1 channel-id Field Descriptions (Specific Channel-ID Selected)

Field	Description
serial interface	Name of the interface serial object and its type (serial or digital).
SCC port	SCC port on the DFC card that was internally assigned by software to service that link (useful to resolve conflicts when trying to create a serial link).
link state	MTP1 link state is started (generally reflects the shutdown and no shutdown entry options.
IDB state	Actual state of the internal Interface Descriptor Block (IDB), which is useful for developers.
rcv-pool	Heading for receive buffer-pool information.
pool-name	Internal name for the pool.
congested	Whether the receive buffers are congested or not.
in-use buffers	How many of the receive buffers are currently in use.
free buffers	How many of the receive buffers are free (not in use).
tx-pool	Heading for transmit buffer-pool information.
pool-name	Internal name for the pool.
in-use buffers	How many of the transmit buffers are currently in use.
free buffers	How many of the transmit buffers are free (not in use).

Related Commands

Command	Description
channel-id	Assigns a session channel ID to an SS7 serial link.
show controllers serial	Displays information about the virtual serial interface.
show ss7 mtp1 links	Displays information for each provisioned SS7 link.

Command	Description
show ss7 mtp2 ccb	Displays SS7 MTP 2 Channel Control Block (CCB) information.
show ss7 mtp2 state	Displays internal SS7 Message Transfer Part level 2 (MTP 2) state machine information.
show ss7 mtp2 stats	Displays SS7 MTP 2 operational statistics.
show ss7 mtp2 timers	Displays durations of the SS7 MTP 2 state machine timers.
show ss7 mtp2 variant	Displays information about the SS7 MTP 2 protocol variant.
show ss7 sm session	Displays information about SS7 Session Manager session.
show ss7 sm set	Displays information about the SS7 failover timer.

show ss7 mtp1 links

To display information for each provisioned Signaling System 7 (SS7) link, use the **show ss7 mtp1 links** command in privileged EXEC mode.

show ss7 mtp1 links

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.2(11)T	This command was introduced on the Cisco AS5350 and Cisco AS5400.
12.2(15)T	This command was implemented on the Cisco 2600 series. Command output was also modified.

Usage Guidelines

Use this command to display the name of the serial interface for the link, the assigned media gateway controller (MGC) port, whether the link is serial (12-in-1 port) or digital (E1/T1 trunk DS0), the assigned channel ID, and whether the link is stopped or started. This command is useful for quickly letting you know what links have been assigned and what channel IDs are in use.

The output for this command has been modified for the Cisco AS5350 and Cisco AS5400 to show SS7 session set information. For the Cisco 2600 series, the SCC and state columns have been removed from the output.

Examples

The following sample output shows that there are four SS7 links (out of a platform maximum of four).

Note The SCC chip number is used by Cisco developers who are checking output from the debug ss7 mtp1 commands.

```
Router# show ss7 mtp1 links
     SS7 MTP1 Links [num = 4, platform max = 4]:
                                          session
       interface  type      SCC  state    channel
       ---------  --------  ---  -------  -------
       7/0:0      digital   7/3  STARTED  0
       7/0:1      digital   7/2  STARTED  1
       7/1:0      digital   7/1  STARTED  2
       7/1:1      digital   7/0  STARTED  3
```

The following example displays the interface, type (serial or digital), SCC port, state (started or stopped), SS7 session set (configured or not), and channel ID for all configured SS7 links on a Cisco AS5350 or Cisco AS5400.

```
Router# show ss7 mtp1 links
 SS7 MTP1 Links [num = 4, platform max = 4]:
                                        session session
```

```
   interface   type   SCC     state    channel   set
   --------- -------- --- ------------ ------- -------
      7/0:0  digital  7/3      STARTED     1       0
      7/0:1  digital  7/2      STOPPED    NA      NA
      7/0:2  digital  7/1      STARTED     3       0
        7/0   serial  7/0      STARTED     0       0
```

The following example displays the interface, type (serial or digital), SS7 session set (configured or not), and channel ID for all configured SS7 links on a Cisco 2611 or Cisco 2651. The SCC and state columns have been removed from the output for these platforms.

```
Router# show ss7 mtp1 links
 SS7 MTP1 Links [num = 4, platform max = 4]:
                      session session
    interface   type   channel   set
    --------- -------- ------- -------
         0/0   serial      0       0
         0/1   serial      1       0
       0/2:0  digital      2       1
       0/3:0  digital      3       1
```

The table below describes significant fields shown in this output.

Table 152: show ss7 mtp1 links Field Descriptions

Field	Description
interface	Name of the serial interface for the link.
type	Type of link: serial or digital.
SCC	Assigned MGC port. The SCC chip number is used by Cisco developers to check output from the **debug ss7 mtp1** command.
State	Whether the link is stopped or started.
channel	Assigned channel ID.
session channel	Assigned channel ID.
session set	Assigned SS7 session number.

Related Commands

Command	Description
channel-id	Assigns a session channel ID to an SS7 serial link.
show controllers serial	Displays information about the virtual serial interface.
show ss7 mtp1 links	Displays information for each provisioned SS7 link.
show ss7 mtp2 ccb	Displays SS7 MTP 2 CCB information.
show ss7 mtp2 state	Displays internal SS7 MTP 2 state machine information.
show ss7 mtp2 stats	Displays SS7 MTP 2 operational statistics.
show ss7 mtp2 timers	Displays durations of the SS7 MTP2 state machine timers.

Command	Description
show ss7 mtp2 variant	Displays information about the SS7 MTP2 protocol variant.
show ss7 sm session	Displays information about an SS7 Session Manager session.
show ss7 sm set	Displays information about the SS7 failover timer.

show ss7 mtp2 ccb

To display Signaling System 7 (SS7) Message Transfer Part level 2 (MTP2) call-control block (CCB) information, use the **show ss7 mtp2 ccb**command in privileged EXEC mode.

show ss7 mtp2 ccb [*channel*]

Syntax Description

channel	(Optional) MTP2 serial channel number. Range is from 0 to 3. Default is 0

Command Default

Channel 0. The default is set when you first configure the MTP2 variant. The link must be out of service when you change the variant.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.0(7)XR	This command was introduced.
12.1(1)T	This command was integrated into Cisco IOS Release 12.1(1)T.
12.3(2)T	The command output was modified to display the following new parameters for the PCR feature: PCR enabled, N2, forced retransmission, and octet count.

Usage Guidelines

The application and meaning of the output is dependent on the MTP2 variant. For example, Japanese Nippon Telephone and Telegraph Cellular System (NTT) and the Japanese Telecommunications Technology Committee (TTC) support only emergency alignment.

Examples

The following is sample output from this command. Output highlighted in bold is for the PCR feature.

```
Router# show ss7 mtp2 ccb 0
SS7 MTP2 Internal Channel Control Block Info for channel 0
Protocol version for channel 0 is Bellcore GR-246-Core Issue 2, Dec 1997
ModuloSeqNumber             = 128   (0x80  )
MaxSeqNumber                = 127   (0x7F  )
Unacked-MSUs (MaxInRTB)     = 127   (0x7F  )
MaxProvingAttempts          = 5     (0x5   )
error_control               = Basic
LSSU_Len                    = 1     (0x1   )
MSU_Len                     = 272   (0x110 )
SUERM-threshold             = 64    (0x40  )
SUERM-number-octets         = 16    (0x10  )
SUERM-number-SUs            = 256   (0x100 )
Tie-AERM-Emergency          = 1     (0x1   )
Tin-AERM-Normal             = 4     (0x4   )
MSU_FISU_Accepted_flag      = TRUE
LSSU_available              = TRUE
AbnormalBSN_flag            = FALSE
AbnormalBSN_flag            = FALSE
UnreasonableBSN             = FALSE
UnreasonableFSN             = FALSE
Abnormal_FIBR_flag          = FALSE
```

```
congestionDiscard           = FALSE
ThisIsA_MSU                 = FALSE
local_processor_outage      = FALSE
remote_processor_outage     = FALSE
provingEmergencyFlag        = TRUE
RemoteProvingEmergencyFlag  = FALSE
further_proving_required    = FALSE
ForceRetransmitFlag         = FALSE
RetransmissionFlag          = FALSE
link_present                = TRUE
Debug Mask                  = 0x0
TX Refc RTB Busy            = 0
TX Refc XTB Fault           = 0
TX Too Long Lost            = 0
TX Enqueue Too Large        = 0
TX Enqueue Failed           = 0
TX CountRTBSlotFull         = 0
TX MaxMSUinXTB              = 0
PCR Enabled                   = TRUE
Forced Retransmission Enabled = TRUE
Forced Retransmission Counts  = 0
N2 Threshhold                 = 4500 octets
N2 Octet-count                = 0 octets
SS7 MTP2 Statistics for channel 0
Protocol version for channel 0 is Bellcore GR-246-Core Issue 2, Dec 1997
OMIACAlignAttemptCount  = 0
OMIACAlignFailCount     = 0
OMIACAlignCompleteCount = 0
OMMSU_TO_XMIT_Count     = 0
OMMSU_XMIT_Count        = 0
OMMSU_RE_XMIT_Count     = 0
OMMSU_RCV_Count         = 0
OMMSU_Posted_Count      = 0
OMMSU_too_long          = 0
OMFISU_XMIT_Count       = 0
OMFISU_RCV_Count        = 0

OMLSSU_XMIT_Count       = 6670
OMLSSU_XMIT_SINCount    = 0
OMLSSU_XMIT_SIECount    = 0
OMLSSU_XMIT_SIOCount    = 6670
OMLSSU_XMIT_SIOSCount   = 0
OMLSSU_XMIT_SIPOCount   = 0
OMLSSU_XMIT_SIBCount    = 0
OMLSSU_RCV_Count        = 0
OMLSSU_RCV_SINCount     = 0
OMLSSU_RCV_SIECount     = 0
OMLSSU_RCV_SIOCount     = 0
OMLSSU_RCV_SIOSCount    = 0
OMLSSU_RCV_SIPOCount    = 0
OMLSSU_RCV_SIBCount     = 0
OMLSSU_RCV_InvalidCount = 0
OMRemote_PO_Count       = 0
OMRemote_Congestion_Cnt = 0
OMtimeINSV (secs)       = 0
OMtimeNotINSV (secs)    = 8
OMMSUBytesTransmitted   = 0
OMMSUBytesReceived      = 0
OMTransmitReqCount      = 7678
OMPDU_notAcceptedCount  = 0
OMPDU_NACK_Count        = 0
OMunreasonableFSN_rcvd  = 0
OMunreasonableBSN_rcvd  = 0
OMT1_TMO_Count          = 0
```

```
OMT2_TMO_Count          = 1
OMT3_TMO_Count          = 0
OMT4_TMO_Count          = 0
OMT5_TMO_Count          = 0
OMT6_TMO_Count          = 0
OMT7_TMO_Count          = 0
OMT8_TMO_Count          = 0
OMTA_TMO_Count          = 0
OMTF_TMO_Count          = 0
OMTO_TMO_Count          = 0
OMTS_TMO_Count          = 0
OMLostTimerCount        = 0
OMOMLostBackHaulMsgs    = 0
OMAERMCount             = 0
OMAERMFailCount         = 0
OMSUERMCount            = 0
OMSUERMFailCount        = 0
OMCongestionCount       = 0
OMCongestionBackhaulCnt = 0
```

The table below describes significant fields shown in this output.

Table 153: show ss7 mtp2 ccb Field Descriptions

Field	Description	Possible Values
PCR Enabled	Whether the error-correction method is set to PCR.	TRUE indicates that PCR is enabled. FALSE indicates that PCR is disabled.
Forced Retransmission	Whether forced retransmission is enabled or disabled.	TRUE indicates that forced-retransmission is enabled. FALSE indicates that forced-retransmission is disabled.
N2 Threshold N2 Octet-count	Status of the N2 parameter and maximum octets available. Number of octets stored in the RTB for an SS7 signaling channel.	--

Related Commands

Command	Description
show ss7 mtp2 state	Displays internal SS7 MTP2 state machine information.

show ss7 mtp2 state

To display internal Signaling System 7 (SS7) Message Transfer Part level 2 (MTP2) state-machine information, use the **show ss7 mtp2 state**command in privileged EXEC mode.

show ss7 mtp2 state [*channel*]

Syntax Description

channel	(Optional) MTP2 serial channel number. Range is from 0 to 3. Default is 0.

Command Default

Information for all channels is displayed.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.0(7)XR	This command was introduced.
12.1(1)T	This command was integrated into Cisco IOS Release 12.1(1)T.
12.3(2)T	The command output was modified to display the following new parameters: PCR enabled and forced retransmission.

Examples

The following example displays the current state of forced retransmission and PCR-enabled flags (shown in bold in the output below):

```
Router# show ss7 mtp2 state 0

SS7 MTP2 states for channel 0
Protocol version for channel 0 is ITU-T Q.703 (1996) (White Book)
  MTP2LSC_INSERVICE       MTP2IAC_IDLE
  MTP2TXC_INSERVICE       MTP2RC_INSERVICE
  MTP2SUERM_MONITORING    MTP2AERM_IDLE
  MTP2CONGESTION_IDLE
    Congestion Backhaul  = Abate
Remote Processor Outage  = FALSE
Forced Retransmission    = FALSE
PCR Enabled              = TRUE
N2                       = 800
```

The following is sample output from this command displaying MTP2 state machine information for two different channels:

```
Router# show ss7 mtp2 state 0
SS7 MTP2 states for channel 0
Protocol version for channel 0 is Japan NTT Q.703 Version 1-1
  MTP2LSC_OOS             MTP2IAC_IDLE
  MTP2TXC_INSERVICE       MTP2RC_IDLE
  MTP2SUERM_IDLE          MTP2AERM_IDLE
  MTP2CONGESTION_IDLE
    Congestion Backhaul  = Abate
Remote Processor Outage  = FALSE
```

```
Router# show ss7 mtp2 state 1
SS7 MTP2 states for channel 1
Protocol version for channel 1 is Japan NTT Q.703 Version 1-1
  MTP2LSC_OOS             MTP2IAC_IDLE
  MTP2TXC_INSERVICE       MTP2RC_IDLE
  MTP2SUERM_IDLE          MTP2AERM_IDLE
  MTP2CONGESTION_IDLE
    Congestion Backhaul  = Abate
Remote Processor Outage  = FALSE
```

The table below describes significant fields shown in this output.

Table 154: show ss7 mtp2 state Field Descriptions

State	Description	Possible Values
MTP2LSC	Overall status of the link.	OOS--Link is out of service. INITIAL_ALIGNMENT--Link is in a transitional link alignment state. ALIGNED_READY--Link is in a transitional link alignment state. ALIGNED_NOT_READY--Link is in a transitional link alignment state. INSERVICE--Link is in service. PROCESSOR_OUTAGE--There is an outage in the local processor. This state implies that the link has been aligned. POWER_OFF--It is possible you don't have the I/O memory set to at least 40 percent. There may not be enough memory for the SS7 MTP2 signaling.
MTP2IAC	Status of the initial alignment control state machine.	IDLE--State machine is idle. It is not aligning the link. NOT_ALIGNED--State machine has begun the alignment process. ALIGNED-- Link has exchanged the alignment handshake with the remote device. PROVING--Link alignment is being proven. This is a waiting period before the LSC state changes to INSERVICE.
MTP2TXC	Status of the transmission control state machine.	IDLE--State machine is inactive. INSERVICE--State machine is the active transmitter.
MTP2RC	Status of the receive control state machine.	IDLE--State machine is inactive. INSERVICE--State machine is the active receiver.

State	Description	Possible Values
MTP2SUERM	Status of the signal unit error monitor (SUERM).	IDLE--State machine is inactive. MONITORING--SUERM is active. SUERM uses a leaky-bucket algorithm to track link errors while the link is in service. If the number of link errors reaches the threshold, the link is taken out of service.
MTP2AERM	Status of the alignment error rate monitor state machine (AERM).	IDLE--State machine is inactive. MONITORING--Alignment error monitor is active. This is part of the alignment process.
MTP2CONGESTION	Status of the congestion control state machine.	IDLE--State machine is inactive. No congestion is detected; normal traffic flow. ACTIVE--Congestion has been declared. The Cisco 2600 series router is sending SIBs every T5, which indicates that the remote end should stop sending new MSUs until the local Cisco 2600 series router can catch up.
Congestion Backhaul	Congestion status of the backhaul link between the Cisco SLT and the media gateway controller.	Abate--Link between the Cisco 2600 series router and the media gateway controller is not under congestion. Onset--Link between the Cisco 2600 series router and the media gateway controller is under congestion. and the Media Gateway Controller should stop sending new MSUs until the local Cisco 2600 series router can catch up.
Remote Processor Outage	Processor outage status of the remote.	TRUE indicates that the remote is in processor outage. FALSE indicates that the remote has not declared processor outage.
Forced Retransmission	Whether forced retransmission is enabled or disabled.	TRUE--Indicates that forced retransmission is enabled. FALSE--Indicates that forced retransmission is disabled.
PCR Enabled	Whether the error-correction method is set to PCR.	TRUE--Indicates that PCR is enabled. FALSE--Indicates that PCR is disabled.
N2	Status of the N2 parameter.	Octet counts are specified.

Related Commands

Command	Description
show ss7 mtp2 ccb	Displays SS7 MTP2 CCB information.

show ss7 mtp2 stats

To display Signaling System 7 (SS7) Message Transfer Part level 2 (MTP2) operational statistics, use the **show ss7 mtp2 stats** command in privileged EXEC mode.

show ss7 mtp2 stats [*channel*]

Syntax Description

channel	(Optional) Specific channel. Range is from 0 to 3.

Command Default

Information for all channels is displayed.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.0(7)XR	This command was introduced.
12.1(1)T	This command was integrated into Cisco IOS Release 12.1(1)T.

Examples

The following is sample output from this command showing operations and maintenance (OM) statistics for MTP2 channel 0:

```
Router# show ss7 mtp2 stats 0
SS7 MTP2 Statistics for channel 0
Protocol version for channel 0 is Japan NTT Q.703 Version 1-1
OMIACAlignAttemptCount  = 0
OMIACAlignFailCount     = 0
OMIACAlignCompleteCount = 0
OMMSU_TO_XMIT_Count     = 0
OMMSU_XMIT_Count        = 0
OMMSU_RE_XMIT_Count     = 0
OMMSU_RCV_Count         = 0
OMMSU_Posted_Count      = 0
OMMSU_too_long          = 0
OMFISU_XMIT_Count       = 0
OMFISU_RCV_Count        = 0
OMLSSU_XMIT_Count       = 17
OMLSSU_XMIT_SINCount    = 0
OMLSSU_XMIT_SIECount    = 0
OMLSSU_XMIT_SIOCount    = 0
OMLSSU_XMIT_SIOSCount   = 17
OMLSSU_XMIT_SIPOCount   = 0
OMLSSU_XMIT_SIBCount    = 0
OMLSSU_RCV_Count        = 0
OMLSSU_RCV_SINCount     = 0
OMLSSU_RCV_SIECount     = 0
OMLSSU_RCV_SIOCount     = 0
OMLSSU_RCV_SIOSCount    = 0
OMLSSU_RCV_SIPOCount    = 0
OMLSSU_RCV_SIBCount     = 0
OMLSSU_RCV_InvalidCount = 0
OMRemote_PO_Count       = 0
OMRemote_Congestion_Cnt = 0
```

```
OMtimeINSV (secs)       = 0
OMtimeNotINSV (secs)    = 9550
OMMSUBytesTransmitted   = 0
OMMSUBytesReceived      = 0
OMTransmitReqCount      = 33
OMPDU_notAcceptedCount  = 0
OMPDU_NACK_Count        = 0
OMunreasonableFSN_rcvd  = 0
OMunreasonableBSN_rcvd  = 0
OMT1_TMO_Count          = 0
OMT2_TMO_Count          = 0
OMT3_TMO_Count          = 0
OMT4_TMO_Count          = 0
OMT5_TMO_Count          = 0
OMT6_TMO_Count          = 0
OMT7_TMO_Count          = 0
OMT8_TMO_Count          = 0
OMTA_TMO_Count          = 0
OMTF_TMO_Count          = 0
OMTO_TMO_Count          = 0
OMTS_TMO_Count          = 477218
OMLostTimerCount        = 0
OMOMLostBackHaulMsgs    = 0
OMAERMCount             = 0
OMAERMFailCount         = 0
OMSUERMCount            = 0
OMSUERMFailCount        = 0
OMCongestionCount       = 0
OMCongestionBackhaulCnt = 0
```

The table below describes significant fields shown in this output.

Table 155: show ss7 mtp2 stats Field Descriptions

Field	Description
OMIACAlignAttemptCount OMIACAlignFailCount OMIACAlignCompleteCount	Counts for Initial Alignment Control (IAC) attempts.
OMMSU_TO_XMIT_Count	Related to the results of the **show ss7 sm stats** command's PDU_pkts_recieve_count statistic. The number shown in OMMSU_TO_XMIT_Count is less than the PDU_pkts_recieve_count because OMMSU_TO_XMIT_Count shows the number of PDUs going out on the link, while the PDU_pkts_recieve_count includes PDUs that are internal to MTP2.
OMMSU_RCV_Count	Related to the results of the **show ss7 sm stats** command's packets_send_count.

Field	Description
OMLSSU_XMIT_Count OMLSSU_XMIT_SINCount OMLSSU_XMIT_SIECount OMLSSU_XMIT_SIOCount OMLSSU_XMIT_SIOSCount OMLSSU_XMIT_SIPOCount OMLSSU_XMIT_SIBCount	Number of times that MTP 2 has posted the specific Link Status Signal Unit (LSSU) to MTP 1. They do *not* show the number of LSSUs actually sent over the link.
OMLSSU_RCV_Count OMLSSU_RCV_SINCount OMLSSU_RCV_SIECount OMLSSU_RCV_SIOCount OMLSSU_RCV_SIOSCount OMLSSU_RCV_SIPOCount OMLSSU_RCV_SIBCount OMLSSU_RCV_InvalidCount	Number of LSSUs received by MTP 2 from MTP 1. Because of MTP 1 filtering, this is *not* the same as the actual LSSUs sent over the link.
OMT1_TMO_Count OMT2_TMO_Count OMT3_TMO_Count OMT4_TMO_Count OMT5_TMO_Count OMT6_TMO_Count OMT7_TMO_Count OMT8_TMO_Count OMTA_TMO_Count OMTF_TMO_Count OMTO_TMO_Count OMTA_TMO_Count OMLostTimerCount	Information about timers in use.
OMLostBackhaulMsgs	How many messages received from the Media Gateway Controller have been lost because of a lack of resources in the Cisco 2600 series router. This count is related to the results of the **show ss7 sm stats** command's PDU_pkts_recieve_count statistic. For example, if the Media Gateway Controller sends 100 MSUs and the Cisco 2600 series router only has 65 free buffers, 35 MSUs might be lost.

Related Commands

Command	Description
show ss7 mtp2 ccb	Displays SS7 MTP2 CCB information.
show ss7 mtp2 state	Displays SS7 MTP2 state-machine information.
show ss7 mtp2 timer	Displays durations of the SS7 MTP2 state-machine timers.
show ss7 mtp2 variant	Displays information about the SS7 MTP2 protocol variant.

show ss7 mtp2 timer

To display durations of the Signaling System 7 (SS7) Message Transfer Part level 2 (MTP2) state-machine timers, use theshow ss7 mtp2 timer command in privileged EXEC mode.

show ss7 mtp2 timer [*channel*]

Syntax Description

channel	(Optional) Specific channel. Range is from 0 to 3.

Command Default

Information for all sessions is displayed.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.0(7)XR	This command was introduced.
12.1(1)T	This command was integrated into Cisco IOS Release 12.1(1)T.

Usage Guidelines

MTP2 uses eight different timers on each link. Throughout the link-state transitions, multiple timers are active. An in-service MTP2 link requires timers that are constantly started, stopped, and restarted. Use this command to display the configured timer durations.

Note All MTP2 configuration parameters are set at the Cisco SLT command-line interface. Media gateway controller parameter data files are no longer used to configure the Cisco SLT.

Note The eight timers whose status is displayed using this command are set on the media gateway controller using MML commands. The timers are then downloaded from the controller to the Cisco signaling link terminal (SLT).

Examples

The following is sample output from this command displaying timer information for channel 0:

```
Router# show ss7 mtp2 timer 0
SS7 MTP2 Timers for channel 0 in milliseconds
Protocol version for channel 0 is Japan NTT Q.703 Version 1-1
    T1 aligned/ready = 15000
      T2 not aligned = 5000
          T3 aligned = 3000
T4 Emergency Proving = 3000
   T4 Normal Proving = 3000
      T5 sending SIB = 200
      T6 remote cong = 3000
 T7 excess ack delay = 2000
  T8 errored int mon = 0
```

```
TA SIE timer = 20
       TF FISU timer = 20
        TO SIO timer = 20
       TS SIOS timer = 20
```

Field descriptions should be self-explanatory.

Related Commands

Command	Description
show ss7 mtp2 ccb	Displays SS7 MTP2 CCB information.
show ss7 mtp2 state	Displays SS7 MTP2 state-machine information.
show ss7 mtp2 stats	Displays SS7 MTP2 operational statistics.
show ss7 mtp2 variant	Displays information about the SS7 MTP2 protocol variant.

show ss7 mtp2 variant

To display information about the Signaling System 7 (SS7) Message Transfer Part level 2 (MTP2) protocol variant, use theshow ss7 mtp2 variant command in privileged EXEC mode.

show ss7 mtp2 variant [*channel*]

Syntax Description

channel	(Optional) Specific channel. Range is from 0 to 3.

Command Default

Information for all channels is displayed.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.0(7)XR	This command was introduced.
12.1(1)T	This command was integrated into Cisco IOS Release 12.1(1)T.
12.2(11)T	This command was integrated into Cisco IOS Release 12.2(11)T and implemented on the Cisco AS5350 and Cisco AS5400.

Usage Guidelines

This command can take an optional channel ID at the end (for example, show ss7 mtp2 variant 0). If the optional channel ID is omitted, the command displays the SS7 variant for all configured SS7 links.

Each country specifies its own variant of SS7, and the Cisco SLT supports several variants of the MTP2 protocol. The selected variant can affect the MTP2 statistics displayed by various commands. The Cisco SLT support the following variants:

- Telcordia Technologies (formerly Bellcore)
- ITU: International Telecommunication Union
- NTT: Japanese Nippon Telephone and Telegraph Cellular System
- TTC: Japanese Telecommunications Technology Committee

Each channel can be configured to any one of the protocol variants. When you change from one variant to another, for example from Bellcore to NTT, the MTP2 parameters default to those specified by NTT. You can then change the defaults as required.

Examples

The following is sample output from this command showing protocol-variant information for channel 1:

```
Router# show ss7 mtp2 variant 1
Protocol version for channel 1 is Bellcore GR-246-Core Issue 2, Dec 1997
```

The following is sample output showing the SS7 variant for the SS7 link whose channel ID is 2:

```
Router# show ss7 mtp2 variant 2
Protocol version for channel 2 is Bellcore GR-246-Core Issue 2, Dec 1997
```

The following is sample output showing the SS7 variant for all configured links:

```
Router# show ss7 mtp2 variant
Protocol version for channel 0 is Bellcore GR-246-Core Issue 2, Dec 1997
Protocol version for channel 1 is Bellcore GR-246-Core Issue 2, Dec 1997
Protocol version for channel 2 is Bellcore GR-246-Core Issue 2, Dec 1997
Protocol version for channel 3 is Bellcore GR-246-Core Issue 2, Dec 1997
```

Field descriptions should be self-explanatory. Note, however, the following:

- In each case, all SS7 links are clearly provisioned to use the Bellcore variant (see the ss7 mtp2 variant bellcore command).
- Command output shows that the MTP2 variant is being used for each of the SS7 links and that the Telcordia Technologies (formerly Bellcore) version is implemented; it also shows where the links are identified by their assigned channel IDs.

Related Commands

Command	Description
show controllers serial	Displays information about the virtual serial interface.
show ss7 mtp1 channel-id	Displays information for a given session channel ID.
show ss7 mtp2 ccb	Displays SS7 MTP 2 CCB information.
show ss7 mtp2 state	Displays internal SS7 MTP 2 state machine information.
show ss7 mtp2 stats	Displays SS7 MTP 2 operational statistics.
show ss7 mtp2 timers	Displays durations of the SS7 MTP 2 state machine timers.
show ss7 sm session	Displays information about SS7 Session Manager session.
show ss7 sm set	Displays information about the SS7 failover timer.
show ss7 mtp2 ccb	Displays SS7 MTP 2 CCB information.
show ss7 mtp2 state	Displays internal SS7 MTP 2 state machine information.
show ss7 mtp2 stats	Displays SS7 MTP 2 operational statistics.
ss7 mtp2 variant bellcore	Configures the device for Telcordia Technologies (formerly Bellcore) standards.

show ss7 sm session

To display information about a Signaling System 7 (SS7) Session Manager session, use the show ss7 sm session command in privileged EXEC mode.

show ss7 sm session [*session*]

Syntax Description

session	(Optional) Session. Range is from 0 to 3.

Command Default

Information for all sessions is displayed.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.0(7)XR	This command was introduced.
12.1(1)T	This command was integrated into Cisco IOS Release 12.1(1)T.
12.2(11)T	This command was integrated into Cisco IOS Release 12.2(11)T. Support for up to four Session Manager sessions was added.

Usage Guidelines

If no sessions are configured, the message "No Session is configured" appears.

Support for up to four Session Manager sessions was added in Cisco IOS Release 12.2(11)T. Session Manager sessions are now numbered from 0 to 3. The Cisco Signalling Link Terminal Dual Ethernet feature changes the command-line-interface syntax and adds sessions 2 and 3.

Examples

The following is sample output from this command displaying session information for both sessions:

```
Router# show ss7 sm session
Session[0]: Remote Host 255.255.251.254:8060, Local Host 255.255.255.254:8060
      retrans_t = 600
      cumack_t  = 300
      kp_t      = 2000
      m_retrans = 2
      m_cumack  = 3
      m_outseq  = 3
      m_rcvnum  = 32
Session[1]: Remote Host 255.255.251.255:8061, Local Host 255.255.255.254:8061
      retrans_t = 600
      cumack_t  = 300
      kp_t      = 2000
      m_retrans = 2
      m_cumack  = 3
      m_outseq  = 3
      m_rcvnum  = 32
```

The table below describes significant fields shown in this output.

Table 156: show ss7 sm session Field Descriptions

Field	Description
Remote Host, Local Host	IP address and port number for the session.
retrans_t	Retransmission timer value.
cumack_t	Cumulative acknowledgment timer value.
m_cumack	Maximum number of segments that can be received before the RUDP sends an acknowledgment.
m_outseq	Maximum number of out-of-sequence segments that can be received before the RUDP sends an extended acknowledgment.
m_rcvnum	Maximum number of segments that the remote end can send before receiving an acknowledgment.

Related Commands

Command	Description
ss7 session	Establishes a session.
ss7 session retrans_t	Sets the retransmission timer.
ss7 session m_rcvnum	Sets the maximum number of segments that the remote end can send before receiving an acknowledgment.
ss7 session m_outseq	Sets the maximum number of out-of-sequence segments that can be received before the RUDP sends an extended acknowledgment.
ss7 session m_cumack	Sets the maximum number of segments that can be received before the RUDP sends an acknowledgment.
ss7 session cumack_t	Sets the cumulative acknowledgment timer.

show ss7 sm set

To display information about the Signaling System 7 (SS7) session set state, failover timer , member sessions, and SS7 links that belong to an SS7 session set or range of SS7 session sets, use the show ss7 sm set command in privileged EXEC mode.

show ss7 sm set [*ss-id-range*]

Syntax Description

ss -id -range	(Optional) Displays the SS7 session set ID, state, member sessions, and SS7 links that belong to an SS7 session set or range of SS7 session sets.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.0(7)XR	This command was introduced.
12.1(1)T	This command was integrated into Cisco IOS Release 12.1(1)T.
12.2(15)T	The ss - id - range argument was added. This command previously displayed only the failover-timer value and had no arguments.

Usage Guidelines

This command is available on all Cisco Signaling Link Terminal (SLT) platforms.

If the optional ss-id-range argument is omitted, information is displayed for all SS7 session sets. The following are valid SS7 session set ranges. The default is 3 seconds.

1	Selects SS7 session set 1 .
0, 2, 3	Selects SS7 session sets 0, 2, and 3.
0-2	Selects SS7 session sets 0, 1, and 2.
0, 2-3	Selects SS7 session sets 0, 2, and 3.
0, 2	Selects SS7 session sets 0 and 2.

Examples

The following is sample output from this command displaying failover timer information; the failover timer is set to the default of 3 seconds:

```
Router# show ss7 sm set
Session Manager Set
      failover timer = 3 seconds
```

The following example displays the SS7 session set state, failover-timer, member sessions, and SS7 links that belong to a range of SS7 session sets:

```
Router# show ss7 sm set
Session-set:0
```

```
  State          = ACTIVE
  Failover-timer = 5 secs.
  2 Sessions:
    session 0  session-state ACTIVE   remote-host 172.16.0.0:5555
    session 1  session-state STANDBY  remote-host 172.31.255.255:4444
  3 SS7 Links:
       7/0 (ser.)    chan-id 0  variant Bellcore   link-state INSERVICE
       7/0:0 (dig.)  chan-id 1  variant Bellcore   link-state INSERVICE
       7/0:2 (dig.)  chan-id 3  variant Bellcore   link-state INITIAL_ALIGNMENT
Session-set:1
  State          = IDLE
  Failover-timer = 5 secs.
  0 Sessions:
  0 SS7 Links:
Session-set:2
  State          = ACTIVE
  Failover-timer = 5 secs.
  2 Sessions:
    session 2  session-state ACTIVE   remote-host 172.16.0.0:6666
    session 3  session-state STANDBY  remote-host 172.31.255.255:7777
  1 SS7 Links:
       7/0:1 (dig.)  chan-id 2  variant Bellcore   link-state INSERVICE
Session-set:3
  State          = IDLE
  Failover-timer = 5 secs.
0 Sessions:
  0 SS7 Links:
```

The table below describes significant fields in this output.

Table 157: show ss7 sm set Field Descriptions

Field	Description
Session-set:0	One of four SS7 session sets is configured.
State	The session is ACTIVE.
Failover-timer	`The number of seconds is set to 5.`
2 Sessions:	• Session 0--session state is ACTIVE and connected to port 5555 of remote-host 172.16.0.0 • Session 1--session state is STANDBY and connected to port 4444 of remote-host 172.31.255.255
3 SS7 Links:	• SS7 link at serial interface 7/0 has channel ID 0 and current MTP2 link state of INSERVICE. • SS7 link at serial interface 7/0:0 has channel ID 1 and current MTP2 link state of INSERVICE. • SS7 link at serial interface 7/0:2 has channel ID 3 and current MTP2 link state of INITIAL_ALIGNMENT.
Session-set:1	One of four SS7 session sets is configured.
State	The session is IDLE.
Failover-timer	The number is set to 5 seconds.

Field	Description
0 Sessions:	No sessions are configured.
0 SS7 Links:	No SS7 links are configured.
Session-set:2	One of four SS7 session sets is configured.
State	The session is ACTIVE.
Failover-timer	`The number is set to 5 seconds.`
2 Sessions:	• Session 2 is ACTIVE and connected to port 6666 of remote host 172.16.0.0 • Session 3 is STANDBY and connected to port 7777 of remote host 172.31.255.255.
1 SS7 Links :	SS7 link at serial interface 7/0:1 has channel ID 2 and current MTP2 link state of INSERVICE.
Session-set:3	One of four SS7 session sets is configured.
State	The session is IDLE.
Failover-timer	The number is set to 5 seconds.
0 Sessions:	No sessions are configured.
0 SS7 Links:	No SS7 links are configured.

Related Commands

Command	Description
ss7 session	Creates a Reliable User Datagram Protocol (RUDP) session and explicitly adds an RUDP session to a Signaling System 7 (SS7) session set.
ss7 set	Independently selects failover-timer values for each session set and specifies the amount of time that the SS7 Session Manager waits for the active session to recover or for the standby media gateway controller (MGC) to indicate that the Cisco Signaling Link Terminal (SLT) should switch traffic to the standby session.
ss7 set failover timer	Specifies the amount of time that the Session Manager waits for the session to recover before declaring the session inactive.

show ss7 sm stats

To display Signaling System 7 (SS7) Session Manager session statistics, use theshow ss7 sm stats command in privileged EXEC mode.

show ss7 sm stats

Syntax Description

There are no arguments or keywords for this command.

Command Default

The command shows information for both sessions.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.0(7)XR	This command was introduced.
12.1(1)T	This command was integrated into Cisco IOS Release 12.1(1)T.

Usage Guidelines

If no sessions are configured, the message "No Session is configured" appears.

Examples

The following is sample output from this command displaying SS7 Session Manager statistics. The fields are self-explanatory and show information about the session state, protocol data units (PDUs) packets sent and received, and SS7 Reliable User Datagram Protocol (RUDP) performance:

```
Router# show ss7 sm stats
-------------------- Session Manager  --------------------
Session Manager state             = SESSION SET STATE-ACTIVE
Session Manager Up count          = 1
Session Manager Down count        = 0
   lost control packet count      = 0
              lost PDU count      = 0
 failover timer expire count      = 0
 invalid_connection_id_count      = 0
Session[0] statistics  SM SESSION STATE-STANDBY:
Session Down count               = 0
   Open Retry count              = 0
   Total Pkts receive count      = 1
   Active Pkts receive count     = 0
   Standby Pkts receive count    = 1
   PDU Pkts receive count        = 0
   Unknown Pkts receive count    = 0
Pkts send count               = 0
   Pkts requeue count            = 0
    -Pkts window full count      = 0
    -Pkts resource unavail count = 0
    -Pkts enqueue fail count     = 0
   PDUs dropped (Large)          = 0
   PDUs dropped (Empty)          = 0
   RUDP Not Ready Errs           = 0
   RUDP Connection Not Open      = 0
   RUDP Invalid Conn Handle      = 0
   RUDP Unknown Errors           = 0
```

```
   RUDP Unknown Signal           = 0
   NonActive Receive count       = 0
Session[1] statistics  SM SESSION STATE-ACTIVE:
Session Down count               = 0
   Open Retry count              = 0
   Total Pkts receive count      = 2440
   Active Pkts receive count     = 1
   Standby Pkts receive count    = 0
   PDU Pkts receive count        = 2439
   Unknown Pkts receive count    = 0
   Pkts send count               = 2905
   Pkts requeue count            = 0
    -Pkts window full count      = 0
    -Pkts resource unavail count = 0
    -Pkts enqueue fail count     = 0
   PDUs dropped (Large)          = 0
   PDUs dropped (Empty)          = 0
   RUDP Not Ready Errs           = 0
   RUDP Connection Not Open      = 0
   RUDP Invalid Conn Handle      = 0
   RUDP Unknown Errors           = 0
   RUDP Unknown Signal           = 0
   NonActive Receive count       = 0
```

Field descriptions should be self-explanatory.

Related Commands

Command	Description
clear ss7 sm-stats	Clears the counters that track Session Manager statistics for the show ss7 sm stats command.
ss7 session	Establishes a session.

show stcapp buffer-history

To display event logs for SCCP Telephony Control Application (STCAPP) analog voice ports, use the **show stcapp buffer-history**command in privileged EXEC mode.

show stcapp buffer-history {**all** | **port** *port*}

Syntax Description

all	Displays event records for all analog voice ports.
port *port*	Displays event records for only the specified analog voice port. **Note** *Port* syntax is platform-dependent; type ? to determine.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.4(2)T	This command was introduced.

Usage Guidelines

To display event logs with this command, you must first enable event logging using the **debug voip application stcapp buffer-history** command.

Note Using the **all** keyword with this command could increase CPU utilization by as much as 40%.

Examples

The following is sample output from the **show sctapp buffer-history** command showing voice port 2/3 registering with the call-control system, going offhook, and then disconnecting:

```
Router# show stcapp buffer-history port 2/3
1. [2/3], 00:00:44.467
IS [DEVICE_UNREGISTERING] --> IS
2. [2/3], 00:00:44.467
IS [DEVICE_RESETTING] --> OOS
3. [2/3], 00:00:44.467
OOS [DEVICE_DESTROYED] --> STATE_NONE
4. [2/3], 00:00:46.455
STATE_NONE [DEVICE_CREATED] --> OOS
5. [2/3], 00:00:46.455
OOS [DEVICE_REGISTERING] --> INIT
6. [2/3], 00:00:46.607
INIT [STCAPP_DC_EV_DEVICE_REGISTER_DONE] --> INIT
7. [2/3], 00:00:46.607
INIT [STCAPP_DC_EV_DEVICE_CAP_REQ] --> INIT
8. [2/3], 00:00:46.883
INIT [STCAPP_DC_EV_DEVICE_BUTTON_TEMP_RES] --> INIT
9. [2/3], 00:00:46.883
INIT [STCAPP_DC_EV_DEVICE_FORWARD_STAT_RES] --> INIT
10. [2/3], 00:00:47.151
```

```
INIT [STCAPP_DC_EV_DEVICE_LINE_STAT_RES] --> INIT
11. [2/3], 00:00:47.163
INIT [STCAPP_DC_EV_DEVICE_DISPLAY_PROMPT_STATUS] --> INIT
12. [2/3], 00:00:47.419
IS [STCAPP_DC_EV_DEVICE_DEFINE_DATE_TIME_RES] --> IS
13. [2/3], 00:00:57.079
IDLE [STCAPP_DC_EV_DEVICE_CALL_STATE_ONHOOK] --> IDLE
14. [2/3], 00:00:57.079
IDLE [STCAPP_DC_EV_DEVICE_CALL_STATE_ONHOOK] --> IDLE
15. [2/3], 00:00:57.079
IS [STCAPP_DC_EV_DEVICE_SET_LAMP] --> IS
16. [2/3], 00:00:57.079
IS [STCAPP_DC_EV_DEVICE_SET_LAMP] --> IS
17. [2/3], 00:06:00.923
IDLE [STCAPP_CC_EV_CALL_SETUP_IND] --> OFFHOOK
18. [2/3], 00:06:01.019
OFFHOOK [STCAPP_DC_EV_DEVICE_CALL_STATE_OFFHOOK (245)] --> OFFHOOK
19. [2/3], 00:06:01.023
IS [STCAPP_DC_EV_DEVICE_DISPLAY_PROMPT_STATUS] --> IS
20. [2/3], 00:06:01.023
OFFHOOK [STCAPP_DC_EV_DEVICE_START_TONE (245)] --> OFFHOOK
21. [2/3], 00:06:01.023
OFFHOOK [STCAPP_CC_EV_CALL_REPORT_DIGITS_DONE] --> OFFHOOK
22. [2/3], 00:06:03.083
OFFHOOK [STCAPP_CC_EV_CALL_DISCONNECTED] --> ONHOOK_DISCONNECT
23. [2/3], 00:06:03.295
IS [STCAPP_DC_EV_DEVICE_DISPLAY_PROMPT_STATUS] --> IS
24. [2/3], 00:06:03.295
ONHOOK_DISCONNECT [STCAPP_DC_EV_DEVICE_CALL_STATE_ONHOOK (245)] --> IDLE
25. [2/3], 00:06:03.299
IDLE [STCAPP_DC_EV_DEVICE_STOP_TONE (245)] --> IDLE
26. [2/3], 00:06:03.303
IDLE [STCAPP_CC_EV_CALL_DISCONNECT_DONE] --> IDLE
```

Related Commands

Command	Description
debug voip application stcapp buffer-history	Enables event logging for STCAPP analog voice ports.
show stcapp statistics	Displays call statistics for STCAPP analog voice ports.

show stcapp device

To display configuration information about Skinny Client Control Protocol (SCCP) telephony control (STC) application (STCAPP) analog voice ports, use the **show stcapp device** command in privileged EXEC mode.

show stcapp device {**name** *device-name* | **summary** | **voice-port** *port*}

Syntax Description

name *device-name*	Displays information for the analog voice port with the specified device name. The device name is the unique device ID that is assigned to the port when it registers with the call-control system.
summary	Displays a summary of all voice ports.
voice-port *port*	Displays information for the specified analog voice port. **Note** The *port* syntax is platform-dependent; type ? to determine appropriate port numbering.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.3(14)T	This command was introduced.
12.4(2)T	This command was modified. Command output was enhanced to display call control block (CCB) and call-control device information.
12.4(4)T	This command was modified. Command output was enhanced to display supported modem transport capability.
12.4(6)XE	This command was modified. Command output was enhanced to display visual message waiting indicator (VMWI) and information for Dial Tone After Remote Onhook feature.
12.4(11)T	This command was integrated into Cisco IOS Release 12.4(11)T.
12.4(22)T	This command was modified. Command output was updated to show IPv6 information.
15.0(1)XA	This command was modified. Cancel Call Waiting information was added to the command output.
15.1(1)T	This command was integrated into Cisco IOS Release 15.1(1)T.
15.1(3)T	This command was modified. Command output was enhanced to display the call waiting tone configuration.

Usage Guidelines

Use this command to display configuration and voice interface card (VIC)-specific port information. The Active Call Info field is populated only if a call is active on the voice port.

Examples

The following is a sample output showing IPv6 addresses for the local and remote sites:

```
Router# show stcapp device voice-port 2/0
Port Identifier: 2/0
Device Type: ALG
Device Id: 1
Device Name: AN1AE2853624400
Device Security Mode : None
Modem Capability: None
Device State: IS
Diagnostic: None
Directory Number: 1000
Dial Peer(s): 1000
Dialtone after remote onhook feature: activated
Busytone after remote onhook feature: not activated
Last Event: STCAPP_DC_EV_DEVICE_CALL_INFO
Line State: ACTIVE
Hook State: OFFHOOK
mwi: DISABLE
vmwi: OFF
PLAR: DISABLE
Number of CCBs: 1
Global call info:
Total CCB count = 2
Total call leg count = 4
Call State for Connection 1: TsConnected
Connected Call Info:
Call Reference: 22690511
Local IPv6 Addr: 2001:DB8:C18:1:218:FEFF:FE71:2AB6
Local IP Port: 17424
Remote IPv6 Addr: 2001:DB8:C18:1:218:FEFF:FE71:2AB6
Remote IP Port: 18282
Calling Number: 1000
Called Number:
Codec: g729br8
SRTP: off
```

The following is a sample output from the **show stcapp device** command for an SCCP analog port with VMWI while the Dial Tone After Remote Onhook Feature is activated:

```
Router# show stcapp device voice-port 2/4
Port Identifier:  2/4
Device Type:      ALG
Device Id:        4
Device Name:      AN0C863967C9404
Modem Capability: None
Device State:     IS
Diagnostic:       None
Directory Number: 7204
Dial Peer(s):     4
Dialtone after remote onhook feature: activated
Last Event:       STCAPP_CC_EV_CALL_DISCONNECT_DONE
Line State:       IDLE
Hook State:       ONHOOK
mwi:              ENABLE
vmwi:             ON
PLAR:             DISABLE
Number of CCBs:   0
```

The following is a sample output from the **show stcapp device** command for an STCAPP analog voice port on a VIC2-2FXS voice interface card specified by the port number:

```
Router# show stcapp device voice-port 1/0/0
Port Identifier:  1/0/0
Device Type:      ALG
Device Id:        3
Device Name:      AN1EBEEB6070200
Device Security Mode : None
Modem Capability: None
Device State:     IS
Diagnostic:       None
Directory Number: 2099
Dial Peer(s):     999100
Dialtone after remote onhook feature: activated
Busytone after remote onhook feature: not activated
Last Event:       STCAPP_CC_EV_CALL_DISCONNECT_DONE
Line State:       IDLE
Line Mode:        CALL_BASIC
Hook State:       ONHOOK
ccw_on:           FALSE
mwi:              DISABLE
vmwi:             OFF
PLAR:             DISABLE
Callback State:   DISABLED
Number of CCBs:   0
Global call info:
    Total CCB count      = 0
    Total call leg count = 0
```

The following is a sample output from the **show stcapp device** command for an STCAPP analog voice port:

```
Router# show stcapp device name AN0C863972F5401
Port Identifier:  2/1
Device Type:      ALG
Device Id:        25
Device Name:      AN0C863972F5401
Device State:     IS
Diagnostic:       None
Directory Number: 9101
Dial Peer(s):     2
Last Event:       STCAPP_CC_EV_CALL_MODIFY_DONE
Line State:       ACTIVE
Hook State:       OFFHOOK
Number of CCBs:   1
Global call info:
    Total CCB count      = 3
    Total call leg count = 6
Call State for Connection 1: TsConnected
Connected Call Info:
   Call Reference: 16777509
   Local IP Addr:  10.1.0.1
   Local IP Port:  18768
   Remote IP Addr: 10.1.0.1
   Remote IP Port: 18542
   Calling Number: 9101
   Called Number:  9102
   Codec:          g711ulaw
```

The following is a sample output from the **show stcapp device** command for STCAPP analog voice ports:

```
Router# show stcapp device summary
Total Devices:           24
```

```
Total Calls in Progress: 3
Total Call Legs in Use:  6
Port       Device          Device   Call          Dev  Directory   Dev
Identifier Name            State    State         Type Number      Cntl
---------- --------------- -------- ------------- ---- ----------- ----
2/1        AN0C863972F5401 IS       ACTIVE         ALG  9101       CCM
2/2        AN0C863972F5402 IS       ACTIVE         ALG  9102       CCM
2/3        AN0C863972F5403 IS       ACTIVE         ALG  9103       CCM
2/0        AN0C863972F5400 IS       IDLE           ALG  9100       CCM
2/4        AN0C863972F5404 IS       IDLE           ALG  9104       CCM
2/5        AN0C863972F5405 IS       IDLE           ALG  9105       CCM
2/6        AN0C863972F5406 IS       IDLE           ALG  9106       CCM
2/7        AN0C863972F5407 IS       IDLE           ALG  9107       CCM
2/8        AN0C863972F5408 IS       IDLE           ALG  9108       CCM
2/9        AN0C863972F5409 IS       IDLE           ALG  9109       CCM
2/10       AN0C863972F540A IS       IDLE           ALG  9110       CCM
2/11       AN0C863972F540B IS       IDLE           ALG  9111       CCM
2/12       AN0C863972F540C IS       IDLE           ALG  9112       CCM
2/13       AN0C863972F540D IS       IDLE           ALG  9113       CCM
2/14       AN0C863972F540E IS       IDLE           ALG  9114       CCM
2/15       AN0C863972F540F IS       IDLE           ALG  9115       CCM
2/16       AN0C863972F5410 IS       IDLE           ALG  9116       CCM
2/17       AN0C863972F5411 IS       IDLE           ALG  9117       CCM
2/18       AN0C863972F5412 IS       IDLE           ALG  9118       CCM
2/19       AN0C863972F5413 IS       IDLE           ALG  9119       CCM
2/20       AN0C863972F5414 IS       IDLE           ALG  9120       CCM
2/21       AN0C863972F5415 IS       IDLE           ALG  9121       CCM
2/22       AN0C863972F5416 IS       IDLE           ALG  9122       CCM
2/23       AN0C863972F5417 IS       IDLE           ALG  9123       CCM
```

The following is a sample output from the **show stcapp device** command for an STCAPP analog voice port:

```
Router# show stcapp device name AN0C86385E3D400
Port Identifier: 2/0
Device Type:      ALG
Device Id:        1
Device Name:      AN0C86385E3D400
Device Security Mode : None
Modem Capability: None
Device State:     IS
Diagnostic:       None
Directory Number: 2400
Dial Peer(s):     2000
Dialtone after remote onhook feature: activated
Busytone after remote onhook feature: not activated
Last Event:       STCAPP_DC_EV_DEVICE_DISPLAY_PROMPT_STATUS
Line State:       IDLE
Line Mode:        CALL_BASIC
Hook State:       ONHOOK
mwi:              DISABLE
vmwi:             OFF
mwi config:       Both
Privacy:          Not configured
PLAR:             DISABLE
Callback State:   IDLE
CWT Repetition Interval: 0 second(s)
Number of CCBs:   0
Global call info:
    Total CCB count      = 0
Total call leg count = 0
```

The table below describes the significant fields shown in these displays, in alphabetical order.

Table 158: show stcapp device Field Descriptions

Field	Description
Active Call Info	Displays only when an active call is in progress.
Call Reference	Reference number created by Cisco Unified Communications Manager to track messages associated with a specific call.
Call State	Call processing state: • ACTIVE--Established call connection • IDLE--No call connection • UNREGISTERED--Device is not registered with the Cisco Unified Communications Manager
Called Number	Device called number.
Calling Number	Device calling number.
ccw_on	Displays status of Cancel Call Waiting feature: • False--Inactive on port. • True--Active on port.
Codec	Displays codec type.
CWT Repetition Interval	Displays the call waiting tone configuration.
Dev Cntl	Call-control device that is managing the analog endpoints. CCM represents Cisco Unified Communications Manager. CME represents Cisco Unified Communications Manager Express.
Device Id	Identifier used between the Cisco Unified Communications Manager and gateway to uniquely identify an endpoint.
Device Name	Unique device ID of the analog endpoint. The device ID is derived from an algorithm using the MAC address of the SCCP interface on the voice gateway and the hexadecimal translation of the port's slot number and port number.

Field	Description
Device State	Displays whether device is available for use: • ACTIVE_PENDING--Call is pending certain events before going active. • INFO_RCVD--Call information is received from the Cisco Unified Communications Manager during call setup. • INIT--Waiting to reinitialize. • IS--In service. • OFFHOOK--Device is off-hook. • OFFHOOK_TIMEOUT--Digit timeout occurred while the device is off-hook. • ONHOOK_PENDING--Call is pending certain events before going to the on-hook state. • OOS--Out of service. • PROCEED--Dialed number translation is complete and call setup is in progress. • REM_ONHOOK_PENDING--Call is pending certain events before going to the on-hook state. • RINGING--An incoming call has invoked ringing of the receiving device.
Device Type	Shows phone type: • ALG--Analog. • BRI--ISDN BRI.
Diagnostic	Reason code for a device error condition.
Dial Peer(s)	Dial peer name.
Dialtone after remote onhook feature	Displays feature status: • Activated • Not activated
Directory Number	Assigned to the device by the Cisco Unified Communications Manager.
Last Event	Last event processed by this port.
Local IP Addr	IPv4 address of this gateway used to stream audio using the Real-Time Transport Protocol (RTP).
Local IPv6 Addr	IPv6 address of this gateway used to stream audio using the RTP.

Field	Description
Local IP Port	IP port of this gateway used to stream audio using RTP.
Port Identifier	Identifies the physical voice port.
Remote IP Addr	IPv4 address of the far-end gateway that streams audio using RTP.
Remote IPv6 Addr	IPv6 address of the far-end gateway that streams audio using RTP.
Remote IP Port	IP port of the far-end gateway that streams audio using RTP.
vmwi	Displays LED status: • On • Off

Related Commands

Command	Description
show stcapp statistics	Displays call statistics for STCAPP devices.

show stcapp feature codes

To display current values for feature access codes (FACs), feature speed-dials (FSDs), and feature callback in the SCCP telephony control (STC) application, use the **show stcapp feature codes** command in privileged EXEC mode.

show stcapp feature codes

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.4(2)T	This command was introduced.
12.4(6)T	This command was modified. Speed-dial output was expanded to include number of digits.
12.4(6)XE	This command was modified. This command was enhanced to display standard and feature call-control modes.
12.4(11)T	This command was integrated into Cisco IOS Release 12.4(11)T.
12.4(20)YA	This command was modified. Command output was enhanced to include values for callback and meetme-conference.
12.4(22)T	This command was integrated into Cisco IOS Release 12.4(22)T.
15.0(1)XA	This command was modified. Cancel Call Waiting information was added to the command output.
15.1(1)T	This command was integrated into Cisco IOS Release 15.1(1)T.

Usage Guidelines

This command shows all values for the following in standard and feature mode, depending on the configuration on the Cisco IOS gateway:

- feature access codes (FACs)
- feature speed-dials (FSD)
- feature callback in the STC application

You can enable FACs and FSDs by using the **stcapp feature access-code** and **stcapp feature speed-dial** commands.

You can enable callback by using the **stcapp feature callback** command.

Examples

The following example displays the values for STC application feature codes if FACs and FSDs are not enabled:

```
Router# show stcapp feature codes
```

```
  stcapp feature access-code disabled
  stcapp feature speed-dials disabled
 stxcapp call-control mode is standard
```

The following example shows that feature mode for call-control is enabled:

```
Router# show stcapp feature codes

  stcapp feature speex-dial disabled
  stacapp call-control mode is feature mode
    #1 -- hangup last active call
    #2 - transfer
    #3 - conference
    #4 -- drop last conferee
    #5 -- toggle between two calls
```

The following example displays the default values for all STC application feature codes, including CallBack on Busy and SCCP Meet-Me Conference:

```
Router# show stcapp feature codes

  stcapp feature access-code
    malicious call ID (MCID) ***
    prefix **
    call forward all **1
    call forward cancel **2
    pickup local group **3
    pickup different group **4
    meetme-conference **5
    pickup direct **6
    cancel call waiting **8
  stcapp feature speed-dial
    prefix *
    redial *#
    speeddial number of digit(s) 1
    voicemail *0
    speeddial1 *1
    speeddial2 *2
    speeddial3 *3
    speeddial4 *4
    speeddial5 *5
    speeddial6 *6
    speeddial7 *7
    speeddial8 *8
    speeddial9 *9
  stcapp feature callback
    key #1
    timeout 30
```

The table below describes significant fields shown in the output of this command, in alphabetical order.

Table 159: show stcapp feature codes Field Descriptions

Field	Description
call forward all	FAC prefix plus FAC set by the **call forward all** command.

Field	Description
call forward cancel	FAC prefix plus FAC set by the **call forward cancel**command.
cancel call waiting	FAC prefix plus FAC set by the **cancel-call-waiting**command.
key	Code set for call back on Busy by the **activation-key** command.
meetme-conference	FAC prefix plus FAC set by the **meetme-conference**command.
pickup different group	FAC prefix plus FAC set by the **pickup group** command.
pickup direct	FAC prefix plus FAC set by the **pickup direct**command.
pickup local group	FAC prefix plus FAC set by the **pickup local**command.
prefix	FAC prefix set by the **prefix** (stcapp-fsd) command or by the **prefix (stcapp-fac)**command.
redial	FSD prefix plus FSD code set by the **redial** command.
speeddial number of digit(s)	FSD digit length set by the **digit** command.
speeddial*x*	FSD prefix plus FSD code from the range set by the **speed dial** command.
timeout	Period in seconds for ringing timer set for Call back on Busy by using the **ringing-timeout** command.
voicemail	FSD prefix plus FSD code set by the **voicemail** command.

Related Commands

Command	Description
activation-key	Defines the activation key for Callback on Busy.
call forward all	Designates an STC application feature access code to activate the forwarding of all calls.
call forward cancel	Designates an STC application feature access code to cancel the forwarding of all calls.
digit	Designates the number of digits for STC application feature speed-dial codes.
meetme-conference	Designates an STC application feature access code for meetme-conference.
pickup direct	Designates an STC application feature access code for directed call pickup.
pickup group	Designates an STC application feature access code for group call pickup from another group.
pickup local	Designates an STC application feature access code for group call pickup from the local group.
prefix (stcapp-fac)	Designates a prefix to precede the dialing of an STC application feature access code.

Command	Description
prefix (stcapp-fsd)	Designates a prefix to precede the dialing of an STC application feature speed-dial code.
redial	Designates an STC application feature speed-dial code to dial again the last number that was dialed.
ringing-timeout	Defines ringing timer for Callback on Busy.
speed dial	Designates a range of STC application feature speed-dial codes.
stcapp feature callback	Enables CallBack on Busy and enters the STC application feature callback configuration mode
stcapp feature access-code	Enters STC application feature access code configuration mode to set feature access codes.
stcapp feature speed-dial	Enters STC application feature speed-dial configuration mode to set feature speed-dial codes.
voicemail (stcapp-fsd)	Designates an STC application feature speed-dial code to dial the voice-mail number.

show stcapp statistics

To display call statistics for SCCP Telephony Control Application (STCAPP) voice ports, use the s**how stcapp statistics** command in privileged EXEC mode.

show sctapp statistics [**all** | **voice-port** *port-number*]

Syntax Description

voice-port *port-number*	(Optional) Displays information for a specific voice port. • *port-number*-- Number of the port on the interface. Refer to the appropriate platform manual or online help for port numbers on your networking device.
all	(Optional) Displays a summary of all voice ports.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.3(14)T	This command was introduced.

Usage Guidelines

Use this command to display call statistics for STCAPP voice ports.

Examples

The following is sample output for the **show sctapp statistics**command for STCAPP voice port 1/0/0.1:

```
Router# show stcapp statistics voice-port 1/0/0.1
STCAPP Device/Call Statistics
    OA = Origination Attempts, TA = Termination Attempts
    Err = Call Errors, PE = Call PreEmptions
Port       DevErr   CallOA   CallTA   CallErr  CallPE
---------- -------- -------- -------- -------- --------
1/0/0.1 0        7        0        0        0
```

The following is sample output for the **show stcapp statistics**command for all STCAPP voice ports:

```
Router# show stcapp statistics all
STCAPP Device/Call Statistics
    OA = Origination Attempts, TA = Termination Attempts
    Err = Call Errors, PE = Call PreEmptions
Port       DevErr   CallOA   CallTA   CallErr  CallPE
---------- -------- -------- -------- -------- --------
1/0/0            0        7        0        0        0
1/0/1            0        0        7        0        0
1/0/3            0        0        0        0        0
1/1/0.1          0        0        0        0        0
1/1/1.1          0        0        0        0        0
1/0/2            0        0        0        0        0
```

The table below describes the significant fields shown in the display.

Table 160: show stcapp statistics Field Descriptions

Field	Description
DevErr	Device errors.
CallOA	Call origination attempts.
CallTA	Call termination attempts.
CallErr	Call errors.
CallPE	Call preemptions.

Related Commands

Command	Description
show stcapp device	Displays configuration information about STCAPP voice ports.

show subscription

To display information about Application Subscribe/Notify Layer (ASNL)-based and non-ASNL-based SIP subscriptions, use the show subscription command in user EXEC or privileged EXEC mode.

show subscription {**asnl session** {**active** | **history** [**errors** | **session-id** *session-id* | **url**] | **statistics**} | **sip**} [**summary**]

Syntax Description

asnl session	ASNL-based subscriptions.
active	Active subscriptions
history	ASNL history table in detailed format.
errors	(Optional) Subscription or notification errors available in the history table.
session-id *session-id*	(Optional) Details of subscriptions matched by session id.
url	(Optional) ASNL subscriptions on a per-URL basis.
statistics	ASNL-based subscriptions.
sip	Both ASNL and non-ASNL based subscriptions.
summary	(Optional) ASNL history table in compact format.

Command Default

No default behavior or values.

Command Modes

User EXEC (>)
Privileged EXEC (#)

Command History

Release	Modification
12.3(4)T	This command was introduced.

Usage Guidelines

Use this command to specify options for displaying ASNL and SIP subscription information. If you have a TCL application that uses the SUBSCRIBE and NOTIFY for External Triggers feature, you can use either the show subscription sip or show subscription asnl command to display subscription information. However, the asnl keyword provides more display options.

Examples

The following examples show ASNL-based active subscriptions. The first example displays the information in detail. The second example displays the information in summary form:

```
Router# show subscription asnl session active
ASNL Active Subscription Records Details:
=========================================
Number of active subscriptions: 1
URL: sip:user@10.7.104.88
  Event Name : stress
```

```
  Session ID : 8
  Expiration Time : 50 seconds
  Subscription Duration : 5 seconds
  Protocol : ASNL_PROTO_SIP
  Remote IP address : 10.7.104.88
  Port : 5060
  Call ID : 5
  Total Subscriptions Sent : 1
  Total Subscriptions Received: 0
  Total Notifications Sent : 0
  Total Notifications Received  : 2
  Last response code : ASNL_NOTIFY_RCVD
  Last error code : ASNL_NONE
  First Subscription Time : 10:55:12 UTC Apr 9 2000
  Last Subscription Time : 10:55:12 UTC Apr 9 2000
  First Notify Time : 10:55:12 UTC Apr 9 2000
  Last Notify Time : 10:55:17 UTC Apr 9 2000
  Application that subscribed : stress
  Application receiving notification: stress
Router# show subscription asnl session active summary
ASNL Active Subscription Records Summary:
 ========================================
Number of active subscriptions: 104
SubId      CallId     Proto          URL                                Event
-----      ------     -----          ---                                -----
14090      N/A        ASNL_PROTO_SIP sip:user@10.7.104.88                newstress
14091      N/A        ASNL_PROTO_SIP sip:user@10.7.104.88                newstress
14092      N/A        ASNL_PROTO_SIP sip:user@10.7.104.88                newstress
14093      N/A        ASNL_PROTO_SIP sip:user@10.7.104.88                newstress
14094      N/A        ASNL_PROTO_SIP sip:user@10.7.104.88                newstress
Subscription HISTORY command (detailed display)
Router# show subscription asnl session history
ASNL Subscription History Records Details:
==========================================
Total history records                          = 1
Total error count                              = 0
Total subscription requests sent               = 1
Total subscription requests received           = 0
Total notification requests sent               = 0
Total notification requests received           = 3
URL: sip:user@10.7.104.88
  Event Name : stress
  Session ID : 8
  Expiration Time : 50 seconds
  Subscription Duration : 10 seconds
  Protocol : ASNL_PROTO_SIP
  Remote IP address : 10.7.104.88
  Port : 5060
  Call ID : 5
  Total Subscriptions Sent : 1
  Total Subscriptions Received: 0
  Total Notifications Sent : 0
  Total Notifications Received : 3
  Last response code : ASNL_UNSUBSCRIBE_SUCCESS
  Last error code : ASNL_NONE
  First Subscription Time : 10:55:12 UTC Apr 9 2000
  Last Subscription Time : 10:55:12 UTC Apr 9 2000
  First Notify Time : 10:55:12 UTC Apr 9 2000
  Last Notify Time : 10:55:22 UTC Apr 9 2000
Subscription HISTORY (Summary display)
Router# show subscription asnl session history summary
ASNL Subscription History Records Summary:
==========================================
Total history records = 2
```

```
Total error count = 0
Total subscription requests sent = 2
Total subscription requests received = 0
Total notification requests sent = 0
Total notification requests received = 6
URL                                                 Session ID  Call ID
---              ----------  -------
sip:user@10.7.104.88                                 9           5
sip:user@10.7.104.88                                 8           5
```

The table below describes significant fields in the displays.

Table 161: show subscription Field Descriptions

Field	Description
Last response code	ASNL response codes: ASNL_NONE--Subscription request was initiated. No response has been received from the subscription server. ASNL_SUBSCRIBE_SUCCESS--Subscription request was successful. ASNL_SUBSCRIBE_PENDING--Subscription request has been sent out. Waiting for a response. ASNL_SUBSCRIBE_FAILED--Subscription request failed. ASNL_SUBSCRIBE_SOCKET_ERR--Socket error occurred when the subscription was initiated. ASNL_SUBSCRIBE_REQ_TIMED_OUT_ERR--Subscription request was sent out. No response has been received from the subscription server. ASNL_SUBSCRIBE_CONN_TIMED_OUT_ERR--The client requested a connection to send a SUBSCRIBE request. Connection establishment timed out. Valid for Transmission Control Protocol (TCP) only. ASNL_SUBSCRIBE_DNS_ERR--Domain Name Server (DNS) error occurred when resolving the host name specified in the subscription request. ASNL_SUBSCRIBE_CONN_CREATE_FAILED_ERR--Attempt to create a connection to the subscription server failed. Valid for TCP only.

Field	Description
Last response code (continued)	ASNL_SUBSCRIBE_INTERNAL_CLIENT_ERR--Internal software error occurred while initiating subscription request. ASNL_SUBSCRIBE_RESPONSE_ERR--Invalid response was received from the subscription server for the subscription request from client. ASNL_SUBSCRIBE_EXPIRED--Subscription expired. ASNL_SUBSCRIBE_CLEANUP--Subscription termination initiated from command line interface (CLI). ASNL_UNSUBSCRIBE_SUCCESS--Subscription termination request was successful. ASNL_UNSUBSCRIBE_PENDING--Subscription termination request was sent out. Waiting for a response. ASNL_UNSUBSCRIBE_FAILED --Subscription termination request failed. ASNL_UNSUBSCRIBE_SOCKET_ERR--Socket error occurred when the subscription termination request was initiated. ASNL_UNSUBSCRIBE_REQ_TIMED_OUT_ERR--Subscription termination request was sent out. No response received from the subscription server. ASNL_UNSUBSCRIBE_CONN_TIMED_OUT_ERR--The client requested a connection to send an UNSUBSCRIBE request. Connection establishment timed out. Valid for TCP only. ASNL_UNSUBSCRIBE_CONN_CREATE_FAILED_ERR--Attempt to create a connection to the subscription server failed. Valid for TCP only. ASNL_UNSUBSCRIBE_INTERNAL_ERR--Internal software error occurred when initiating subscription termination request. ASNL_UNSUBSCRIBE_RESPONSE_ERR--Invalid response was received from the subscription server for the subscription termination request from the client. ASNL_NOTIFY_RCVD--Received a notification request from the subscription server.

Field	Description
Last error code	Subscription error codes: ASNL_SUBSCRIBE_PENDING--Subscription request has been sent out. Waiting for a response. ASNL_SUBSCRIBE_FAILED--Subscription request failed. ASNL_SUBSCRIBE_SOCKET_ERR--Socket error occurred when the subscription was initiated. ASNL_SUBSCRIBE_REQ_TIMED_OUT_ERR--Subscription request was sent out. No response has been received from the subscription server. ASNL_SUBSCRIBE_CONN_TIMED_OUT_ERR--The client requested a connection to send a SUBSCRIBE request. Connection establishment timed out. Valid for TCP only. ASNL_SUBSCRIBE_DNS_ERR--DNS error occurred when resolving the host name specified in the subscription request. ASNL_SUBSCRIBE_CONN_CREATE_FAILED_ERR--Attempt to create a connection to the subscription server failed. Valid for TCP only. ASNL_SUBSCRIBE_INTERNAL_CLIENT_ERR--Internal software error occurred while initiating subscription request. ASNL_SUBSCRIBE_RESPONSE_ERR--Invalid response was received from the subscription server for the subscription request from client. ASNL_SUBSCRIBE_EXPIRED--Subscription expired. ASNL_UNSUBSCRIBE_FAILED --Subscription termination request failed. ASNL_UNSUBSCRIBE_SOCKET_ERR--Socket error occurred when the subscription termination request was initiated. ASNL_UNSUBSCRIBE_REQ_TIMED_OUT_ERR--Subscription termination request was sent out. No response received from the subscription server. ASNL_UNSUBSCRIBE_CONN_TIMED_OUT_ERR--The client requested a connection to send an UNSUBSCRIBE request. Connection establishment timed out. Valid for TCP only. ASNL_UNSUBSCRIBE_CONN_CREATE_FAILED_ERR--Attempt to create a connection to the subscription server failed. Valid for TCP only. ASNL_UNSUBSCRIBE_INTERNAL_ERR--Internal software error occurred when initiating subscription termination request. ASNL_UNSUBSCRIBE_RESPONSE_ERR--Invalid response was received from the subscription server for the subscription termination request from the client.

Related Commands

Command	Description
clear subscription	Clears all active subscriptions or a specific subscription.
debug asnl events	Traces event logs in the ASNL.
subscription asnl session history	Specifies how long to keep ASNL subscription history records and how many history records to keep in memory.

Command	Description
subscription maximum	Specifies the maximum number of outstanding subscriptions to be accepted or originated by a gateway.

show subscription local

To show all the LOCAL Subscribe/Notify Service Provider (SNSP) subscriptions, use the **show subscription local** command in privileged EXEC mode.

show subscription local [**aaa**] [**summary**]

Syntax Description

aaa	(Optional) Subscriptions for voice authentication, authorization, and accounting (AAA) server applications under local SNSP.
summary	(Optional) Summary of all subscriptions.

Command Default

All LOCAL SNSP subscriptions are displayed in detailed format.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.3(4)T	This command was introduced.

Usage Guidelines

Use this command to display all the subscriptions for voice AAA server applications under LOCAL SNSP in a detailed or summary format.

Examples

The following is sample output from the **show subscription local**command:

```
Router# show subscription local
ASNL Active Subscription Records Details:
=========================================
Number of active subscriptions:2
URL:local://aaa
  Event Name                  :accounting-notification
  Session ID                  :1
  Expiration Time             :5000 seconds
  Subscription Duration       :0 seconds
  Protocol                    :ASNL_PROTO_LOCAL
  Call ID                     :N/A
  Total Subscriptions Sent    :1
  Total Notifications Received:1
  Last response code          :ASNL_NOTIFY_RCVD
  Last error code             :ASNL_NONE
  First Subscription Time     :00:48:12 UTC Dec 18 2002
  Last Subscription Time      :00:48:12 UTC Dec 18 2002
  First Notify Time           :00:48:12 UTC Dec 18 2002
  Last Notify Time            :00:48:12 UTC Dec 18 2002
  Application that subscribed       :GAS
  Application receiving notification:N/A
URL:local://aaa
  Event Name                  :accounting-notification
  Session ID                  :2
  Expiration Time             :5000 seconds
  Subscription Duration       :0 seconds
  Protocol                    :ASNL_PROTO_LOCAL
```

```
  Call ID                     :N/A
  Total Subscriptions Received:1
  Total Notifications Sent    :1
  Last response code          :ASNL_NOTIFY_ACCEPT
  Last error code             :ASNL_NONE
  First Subscription Time     :00:48:12 UTC Dec 18 2002
  Last Subscription Time      :00:48:12 UTC Dec 18 2002
  First Notify Time           :00:48:12 UTC Dec 18 2002
  Last Notify Time            :00:48:12 UTC Dec 18 2002
  Server Application   :Voice AAA
  notificationMList    :ml1
  notificationPeriod   :limited
  notificationType     :start-update-stop-accounting-on
  reportAcctFailure    :yes
  subscritpion state   :notify_acked
  notification started :no
```

The following is sample output from the **show subscription local aaa**command:

```
Router# show subscription local aaa
ASNL Active Subscription Records Details:
=========================================
Number of active subscriptions:2
URL:local://aaa
  Event Name                  :accounting-notification
  Session ID                  :2
  Expiration Time             :5000 seconds
  Subscription Duration       :140 seconds
  Protocol                    :ASNL_PROTO_LOCAL
  Call ID                     :N/A
  Total Subscriptions Received:1
  Total Notifications Sent    :2
  Last response code          :ASNL_NOTIFY_ACCEPT
  Last error code             :ASNL_NONE
  First Subscription Time     :00:48:12 UTC Dec 18 2002
  Last Subscription Time      :00:48:12 UTC Dec 18 2002
  First Notify Time           :00:48:12 UTC Dec 18 2002
  Last Notify Time            :00:50:32 UTC Dec 18 2002
  Server Application   :Voice AAA
  notificationMList    :ml1
  notificationPeriod   :limited
  notificationType     :start-update-stop-accounting-on
  reportAcctFailure    :yes
  subscritpion state   :notify_acked
  notification started :yes
```

The table below describes significant fields shown in the displays.

Table 162: show subscription local aaa Field Descriptions

Field	Description
Last response code	ASNL response codes. The field can be one of the following values: ASNL_NONE--Subscription request was initiated. No response has been received from the subscription server. ASNL_SUBSCRIBE_SUCCESS--Subscription request was successful. ASNL_SUBSCRIBE_PENDING--Subscription request has been sent out. Waiting for a response. ASNL_SUBSCRIBE_FAILED--Subscription request failed. ASNL_SUBSCRIBE_SOCKET_ERR--Socket error occurred when the subscription was initiated. ASNL_SUBSCRIBE_REQ_TIMED_OUT_ERR--Subscription request was sent out. No response has been received from the subscription server. ASNL_SUBSCRIBE_CONN_TIMED_OUT_ERR--The client requested a connection to send a SUBSCRIBE request. Connection establishment timed out. Valid for Transmission Control Protocol (TCP) only. ASNL_SUBSCRIBE_DNS_ERR--Domain Name Server (DNS) error occurred when resolving the host name specified in the subscription request. ASNL_SUBSCRIBE_CONN_CREATE_FAILED_ERR--Attempt to create a connection to the subscription server failed. Valid for TCP only. ASNL_SUBSCRIBE_INTERNAL_ERR--Internal software error occurred while initiating subscription request. ASNL_SUBSCRIBE_RESPONSE_ERR--Invalid response was received from the subscription server for the subscription request from client. ASNL_SUBSCRIBE_EXPIRED--Subscription expired. ASNL_SUBSCRIBE_CLEANUP--Subscription termination initiated from command line interface (CLI). ASNL_UNSUBSCRIBE_SUCCESS--Subscription termination request was successful. ASNL_UNSUBSCRIBE_PENDING--Subscription termination request was sent out. Waiting for a response. ASNL_UNSUBSCRIBE_FAILED --Subscription termination request failed.
Last response code (continued)	ASNL_UNSUBSCRIBE_SOCKET_ERR--Socket error occurred when the subscription termination request was initiated.

Field	Description
	ASNL_UNSUBSCRIBE_REQ_TIMED_OUT_ERR--Subscription termination request was sent out. No response received from the subscription server. ASNL_UNSUBSCRIBE_CONN_TIMED_OUT_ERR--The client requested a connection to send an UNSUBSCRIBE request. Connection establishment timed out. Valid for TCP only. ASNL_UNSUBSCRIBE_CONN_CREATE_FAILED_ERR--Attempt to create a connection to the subscription server failed. Valid for TCP only. ASNL_UNSUBSCRIBE_INTERNAL_ERR--Internal software error occurred when initiating subscription termination request. ASNL_UNSUBSCRIBE_RESPONSE_ERR--Invalid response was received from the subscription server for the subscription termination request from the client. ASNL_NOTIFY_RCVD--Received a notification request from the subscription server.
Last error code	Subscription error codes. The field can be one of the following values: ASNL_SUBSCRIBE_PENDING--Subscription request has been sent out. Waiting for a response. ASNL_SUBSCRIBE_FAILED--Subscription request failed. ASNL_SUBSCRIBE_SOCKET_ERR--Socket error occurred when the subscription was initiated. ASNL_SUBSCRIBE_REQ_TIMED_OUT_ERR--Subscription request was sent out. No response has been received from the subscription server. ASNL_SUBSCRIBE_CONN_TIMED_OUT_ERR--The client requested a connection to send a SUBSCRIBE request. Connection establishment timed out. Valid for TCP only. ASNL_SUBSCRIBE_DNS_ERR--DNS error occurred when resolving the host name specified in the subscription request. ASNL_SUBSCRIBE_CONN_CREATE_FAILED_ERR--Attempt to create a connection to the subscription server failed. Valid for TCP only. ASNL_SUBSCRIBE_INTERNAL_ERR--Internal software error occurred while initiating subscription request.

Field	Description
Last error code (continued)	ASNL_SUBSCRIBE_RESPONSE_ERR--Invalid response was received from the subscription server for the subscription request from client. ASNL_SUBSCRIBE_EXPIRED--Subscription expired. ASNL_UNSUBSCRIBE_FAILED --Subscription termination request failed. ASNL_UNSUBSCRIBE_SOCKET_ERR--Socket error occurred when the subscription termination request was initiated. ASNL_UNSUBSCRIBE_REQ_TIMED_OUT_ERR--Subscription termination request was sent out. No response received from the subscription server. ASNL_UNSUBSCRIBE_CONN_TIMED_OUT_ERR--The client requested a connection to send an UNSUBSCRIBE request. Connection establishment timed out. Valid for TCP only. ASNL_UNSUBSCRIBE_CONN_CREATE_FAILED_ERR--Attempt to create a connection to the subscription server failed. Valid for TCP only. ASNL_UNSUBSCRIBE_INTERNAL_ERR--Internal software error occurred when initiating subscription termination request. ASNL_UNSUBSCRIBE_RESPONSE_ERR--Invalid response was received from the subscription server for the subscription termination request from the client.
notificationMList	String name of the method list of this subscription.
notificationPeriod	• limited--Notifications are started when the first failure status is received while the server is reachable and stopped when the server changes from unreachable to reachable. • infinite--Notifications are started when the subscription begins and stop only when the subscription expires.
notificationType	Type of accounting record for which notification is sent: start, stop, update, or accounting-on.
reportAcctFailure	Indicates whether to send accounting failure responses to the individual application call script before the method list is declared unreachable.
subscription state	When a subscription is completed successfully, the state is notify_acked.

Related Commands

Command	Description
show subscription	Displays information about ASNL-based and non-ASNL-based SIP subscriptions.

show tbct

To display two b-channel transfer (TBCT) related parameters, use the **show tbct** command in privileged EXEC mode.

show tbct

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
15.0(1)	This command was introduced in a release earlier than Cisco IOS Release 15.0(1).

Examples

The following is sample output from the **show tbct** command. The fields in the output are self-explanatory.

```
Router# show tbct
TBCT:
        Maximum no. of TBCT calls allowed: No limit
        Maximum TBCT call duration: No limit
There are no TBCT calls currently being monitored.
```

Related Commands

Command	Description
tbct clear call	Terminates billing statistics for one or more active TBCT calls.
tbct max calls	Sets the maximum number of active calls that can use TBCT.

show tdm mapping

To display digital signal 0 (DS0) to resource mapping information for a time-division multiplexing (TDM) connection, use the **show tdm mapping** command in user EXEC or privileged EXEC mode.

show tdm mapping [**controller** [**e1** *number*] | **slot** *number*]

Syntax Description

controller	(Optional) Displays information about the T1 or E1 controller.
e1	(Optional) Displays information about the E1 controller.
number	(Optional) Specifies the E1 controller unit number.
slot	(Optional) Displays information about a particular modem card slot.
number	(Optional) Specifies the modem card slot number.

Command Default

If no argument is specified, information for all controllers and slots are displayed.

Command Modes

User EXEC (>)
Privileged EXEC (#)

Command History

Release	Modification
12.4(24)T	This command was introduced in a release earlier than Cisco IOS Release 12.4(24)T.

Examples

The following is sample output from the **show tdm mapping** command. The fields in the display are self-explanatory.

```
Router# show tdm mapping

T1 1/0:1 is up:
Loopback: NONE
DS0      Resource    Call Type
-----------------------------------
 1        Freedm      DATA
 2        Freedm      DATA
 3        Freedm      DATA
 4        Freedm      DATA
 5        Freedm      DATA
 6        Freedm      DATA
 7        Freedm      DATA
 8        Freedm      DATA
 9        Freedm      DATA
10        Freedm      DATA
11        Freedm      DATA
12        Freedm      DATA
13        Freedm      DATA
14        Freedm      DATA
15        Freedm      DATA
16        0            DATA
17        0            DATA
```

```
18        0            DATA
19        0            DATA
20        0            DATA
21        0            DATA
22        0            DATA
23        0            DATA
24        Freedm       Signaling
T1 1/0:2 is up:
Loopback: NONE
DS0      Resource    Call Type
-----------------------------------
 1        Freedm      DATA
 2        Freedm      DATA
 3        Freedm      DATA
 4        Freedm      DATA
 5        Freedm      DATA
 6        Freedm      DATA
 7        Freedm      DATA
 8        Freedm      DATA
 9        Freedm      DATA
10        Freedm      DATA
11        Freedm      DATA
12        Freedm      DATA
13        Freedm      DATA
14        Freedm      DATA
15        Freedm      DATA
16        0            DATA
17        0            DATA
18        0            DATA
19        0            DATA
20        0            DATA
21        0            DATA
22        0            DATA
23        0            DATA
24        Freedm       Signaling
```

Related Commands

Command	Description
show tdm connections	Displays a snapshot of the TDM bus connection memory in a Cisco access server or displays information about the connection memory programmed on the Mitel TDM chip in a Cisco AS5800 access server.

show tgrep neighbors

To display information about the configured Telephony Gateway Registration Protocol (TGREP) neighbors, use the **show tgrep neighbor**s command in privileged EXEC mode.

show tgrep neighbors {***ip-address***}

Syntax Description

*	Displays all neighbors.
ip -address	IP address of the individual neighbor.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.3(1)	This command was introduced.
12.4(24)T	This command was integrated into Cisco IOS Release 12.4(24)T.

Examples

The following is sample output from the **show tgrep neighbors** command:

```
Router# show tgrep neighbors *
There are 1 nbrs configured
------------------ NBR:192.0.2.0----------------------
TIMERS:
        Keepalive :  Timer Stopped
        Hold Timer :  Timer Stopped
        Connect Retry :  Running, time remaining in ms, 20698
SYNC IN PROGRESS
STATE: TRIPS_IDLE
QUEUES:
        writeQ : 0
        sec_writeQ : 0
        readQ : 0
SOCKET FDs:
prim socket -1, sec socket -1
tgrep_update_version : 0
LAST RESET: USER_INITIATED
Router#
Router#!!!! Trip Connection is setup here...
------------------------ OPEN DUMP BEGINS ------------------------
 0x1 0xFFFFFFFF 0x0 0xFFFFFFB4 0x0
 0x0 0x4 0x58 0x6 0x7
 0xFFFFFF98 0xFFFFFFA9 0x0 0xC 0x0
 0x1 0x0 0x8 0x0 0x2
 0x0 0x4 0x0 0x0 0x0
 0x3
        Version    :1
        Hold Time    :180
        My ITAD      :1112
        TRIP ID      :101161129
                 Option Paramater #1
                 Param Type: Capability
```

```
                Length 8
                        Cap Code :Send Receive Capability
                        Cap Len  :4
                               Send Rec Cap: RCV ONLY MODE
        -->All route types supported
------------------------ OPEN DUMP ENDS ------------------------
```

The table below describes the significant fields shown in the display.

Table 163: show tgrep neighbors Field Descriptions

Field	Description
TIMERS	Settings for specified timers.
STATE	State of the connection.
QUEUES	The number of writeQ, sec_writeQ, and readQueues are specified in the following three rows.
SOCKET	Socket field description.
LAST RESET	Last reset state.

Related Commands

Command	Description
neighbor (tgrep)	Creates a TGREP session with another device.

show translation-rule

To display the contents of the rules that have been configured for a specific translation name, use the **show translation-rule** command in privileged EXEC mode.

show translation-rule [*name-tag*]

Syntax Description

name -tag	(Optional) Tag number by which the rule set is referenced. This is an arbitrarily chosen number. Range is from 1 to 2147483647.

Command Default

This command gives detailed information about configured rules under a specific rule name. If the name tag is not entered, a complete display of all the configured rules is shown.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.0(7)XR1	This command was introduced for VoIP on the Cisco AS5300.
12.0(7)XK	This command was implemented for the following voice technologies on the following platforms: • VoIP (Cisco 2600 series, Cisco 3600 series, and Cisco MC3810) • VoFR (Cisco 2600 series, Cisco 3600 series, and Cisco MC3810) • VoATM (Cisco 3600 series and Cisco MC3810)
12.1(1)T	This command was implemented for VoIP on the Cisco 1750, Cisco 2600 series, Cisco 3600 series, Cisco AS5300, Cisco 7200 series, and Cisco 7500.
12.1(2)T	This command was implemented for the following voice technologies on the following platforms: • VoIP (Cisco MC3810) • VoFR (Cisco 2600 series, Cisco 3600 series, and Cisco MC3810) • VoATM (Cisco 3600 series and Cisco MC3810)
12.2(2)XB1	This command was implemented on the Cisco AS5850.
12.2(11)T	This command was integrated into Cisco IOS Release 12.2(11)T.

Examples

The following is sample output from this command:

```
Router# show translation-rule
Translation rule address:0x61AB94F8
Tag name:21
Translation rule in_used 1
```

```
**** Xrule rule table *******
        Rule :1
        in_used state:1
        Match pattern:555.%
        Sub  pattern:1408555
        Match  type:subscriber
        Sub type:international
**** Xrule rule table *******
        Rule :2
        in_used state:1
        Match pattern:8.%
        Sub  pattern:1408555
        Match  type:abbreviated
        Sub type:international
Translation rule address:0x61C2E6D4
Tag name:345
Translation rule in_used 1
**** Xrule rule table *******
        Rule :1
        in_used state:1
        Match pattern:.%555.%
        Sub  pattern:7
        Match  type:ANY
        Sub type:abbreviated
```

The table below describes significant fields in this output.

Table 164: show translation-rule Field Descriptions

Translation rule address	Translation rule address in hex.
Tag name	Translation rule tag name.
Translation rule in_used	Translation rule in which the tag is used.
**** Xrule rule table *******	Beginning of the display for a specific rule.
Rule:x	Number of the rule.
in_used state:	Input-searched-pattern.
Match pattern:	Match pattern of the rule.
Sub pattern:	Substituted pattern.
Match type:	Match type.
Sub type:	Substituted pattern match type.

Related Commands

Command	Description
numbering-type	Specifies number type for the VoIP or POTS dial peer.
rule	Applies a translation rule to a calling party number or a called party number for both incoming and outgoing calls.
test translation-rule	Tests the execution of the translation rules on a specific name-tag.

Command	Description
translate	Applies a translation rule to a calling party number or a called party number for incoming calls.
translate-outgoing	Applies a translation rule to a calling party number or a called party number for outgoing calls.
translation-rule	Creates a translation name and enters translation-rule configuration mode.
voip-incoming translation-rule	Captures calls that originate from H.323-compatible clients.

show trunk group

To display information for one or more trunk groups, use the **show trunk group** command in user EXEC or privileged EXEC mode.

show trunk group [*name* [**cic**] [**sort** [**ascending** | **descending**]]]

Syntax Description

name	(Optional) Trunk group to display.
cic	(Optional) Displays the Circuit Identification Code (CIC) number.
sort	(Optional) Sorts the output by trunk group number, in ascending or descending order.
ascending	(Optional) Specifies ascending display order for the trunk groups. This is the default.
descending	(Optional) Specifies descending display order for the trunk groups.

Command Default

Trunk groups display in ascending order.

Command Modes

User EXEC (>)
Privileged EXEC (#)

Command History

Release	Modification
12.2(11)T	This command was introduced.
12.3(11)T	This command was modified. This command was enhanced to support dial-out trunk groups.
12.4(4)XC	This command was implemented on the Cisco 2600XM series, Cisco 2800 series, Cisco 3700 series, and Cisco 3800 series.
12.4(9)T	This command was integrated into Cisco IOS Release 12.4(9)T.
15.0(1)XA	This command was modified. The output was enhanced to show the logical partitioning class of restriction (LPCOR) policy for incoming and outgoing calls.
12.4(24)T	This command was modified in a release earlier than Cisco IOS Release 12.4(24)T. The **cic**keyword was added.
15.1(1)T	This command was integrated into Cisco IOS Release 15.1(1)T.

Examples

The following sample output shows that for trunk group 1, preemption is enabled, with a preemption tone timer of 10 seconds, and the preemption level is flash.

```
Router# show trunk group 1
Trunk group: 1
        Description:
        trunk group label: 1
        Translation profile (Incoming):
        Translation profile (Outgoing):
```

```
        LPCOR (Incoming): local_group
        LPCOR (Outgoing): local_group
        Preemption is enabled
        Preemption Tone Timer is 10 seconds
        Preemption Guard Timer is 60 milliseconds
        Hunt Scheme is least-used
        Max Calls (Incoming):   NOT-SET (Any)   NOT-SET (Voice) NOT-SET
(Data)
        Max Calls (Outgoing):   NOT-SET (Any)   NOT-SET (Voice) NOT-SET
(Data)
        Retries: 0
        Trunk Se0/3/0:15        Preference DEFAULT
                Member Timeslots : 1-5
                Total channels available : 5
                Data = 0, Voice = 0, Modem = 0, Pending = 0, Free = 5
        Trunk Se0/3/1:15        Preference DEFAULT
                Member Timeslots : 1-2
                Total channels available : 0
                Data = 0, Voice = 0, Modem = 0, Pending = 0, Free = 0
        Trunk Se1/0/0:15        Preference DEFAULT
                Member Timeslots : 1-31
                Total channels available : 0
                Data = 0, Voice = 0, Modem = 0, Pending = 0, Free = 0
        Trunk Se1/0/1:15        Preference DEFAULT
                Member Timeslots : 1-10
                Total channels available : 0
                Data = 0, Voice = 0, Modem = 0, Pending = 0, Free = 0
        Total calls for trunk group: Data = 0, Voice = 0, Modem = 0
                                     Pend = 0, Free = 5
        Preemption Call Type:   Active  Pending
                Flash-Override  NA      0
                Flash           0       0
                Immediate       0       0
                Priority        0       0
                Routine         0       0
                Total           0       0
        Active preemption call-type shows the number of calls
        of each priority level which can be preempted by
        higher preemption level calls.
        Pending preemption call-type shows the number of calls
        of each priority level which are pending for the completion
        of call preemption.
        advertise_flag 0x00000040, capacity timer 25 sec tripl_config_mask 0x00000000
        AC_curr 5, FD_curr 0, SD_curr 0
        succ_curr 0 tot_curr 1
        succ_report 0 tot_report 1
        changed 1 replacement position 0
```

The table below describes the significant fields shown in the output. Fields are listed in alphabetical order.

Table 165: show trunk group Field Descriptions

Field	Description
Description	Description of the trunk group if entered with the **description**(trunk group) command.
trunk group label	Name of the trunk group.
Translation profile (Incoming)	List of incoming translation profiles.

Field	Description
Translation profile (Outgoing)	List of outgoing translation profiles.
LPCOR (Incoming)	Setting of the **lpcor incoming** command.
LPCOR (Outgoing)	Setting of the **lpcor outgoing** command.
Preemption is	Indicates whether preemption is enabled or disabled.
Preemption level	The preemption level for voice calls to be preempted by a DDR call.
Preemption tone timer	The expiry time for the preemption tone for the outgoing calls being preempted by a DDR call.
Hunt Scheme	Name of the idle channel hunt scheme used for this trunk group.
Max calls (incoming)	Maximum number of incoming calls handled by this trunk group.
Max calls (outgoing)	Maximum number of outgoing calls handled by this trunk group.
Retries	Number of times the gateway tries to complete the call on the same trunk group.
Total calls for trunk group	List of the total calls across all trunks in the trunk group.
Preemption Call Type	List of preemption levels for active and pending calls.
Data	Number of currently used data channels on the trunk or total data calls used by the trunk group.
Free	Number of currently available channels on the trunk or total available calls for the trunk group.
Member timeslots	Member timeslots for this trunk.
Pending	Number of pending channels.
Preference	Preference of the trunk in the trunk group. If DEFAULT appears, the trunk does not have a defined preference.
Total channels available	Number of available channels for the trunk.
Trunk group	ID of the trunk group member.
Voice	Number of currently used voice channels on the trunk or total voice calls used by the trunk group.

Related Commands

Command	Description
description (trunk group)	Includes a specific description of the trunk group interface.
hunt-scheme least-idle	Specifies the method for selecting an available incoming or outgoing channel.

Command	Description
trunk group	Initiates a trunk group definition.
trunk group timeslots	Directs an outbound synchronous or asynchronous call initiated by DDR to use specific DS0 channels of an ISDN circuit.

show trunk hdlc

To show the state of the HDLC controllers, use the **show trunk hdlc**command in privileged EXEC mode.

show trunk hdlc {**all** | **ds0** | **slot number**}

Syntax Description

all	Displays information about all the slots with HDLC controllers.
ds0	Displays Ds0 channel availability.
slot	Displays HDLC information about a specific slot.
number	Trunk card slot number.

Command Default

No default behavior or values.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.3(2)T	This command was introduced on the Cisco AS5850.

Usage Guidelines

The output of the command shows the number of calls on each HDLC controller chip and link. If HDLC calls are failing, this command can help determine if the problem is due to a hardware fault and which controller chip may be responsible.

Examples

The following example displays HDLC controller information for all slots:

```
Router# show trunk hdlc all
HDLC Controller information for slot(s): 0 - 13
  Slot 3:
  Sub-   HDLC   HDLC ctrlrs   TDM links (streams): avail DS0s/total DS0s
  slot   Chip   Avail Total   Link0 Link1 Link2 Link3 Link4 Link5 Link6 Link7
  0      0      128   128     31/31 31/31 31/31 31/31 31/31 31/31 31/31  n/a
  0      1      128   128     31/31 31/31 31/31 31/31 31/31 31/31 31/31  n/a
  Slot 12:
  Sub-   HDLC   HDLC ctrlrs   TDM links (streams): avail DS0s/total DS0s
  slot   Chip   Avail Total   Link0 Link1 Link2 Link3 Link4 Link5 Link6 Link7
  0      0      124   124     31/31 31/31 31/31 31/31  n/a   n/a   n/a   n/a
  0      1      124   124     31/31 31/31 31/31 31/31  n/a   n/a   n/a   n/a
```

Table 166: show trunk hdlc Field Descriptions

Field	Description
Subslot	The DFC slot number upon which the controller resides
HDLC Chip	The chip number within the subslot

Field	Description
HDLC available	The number of HDLC channels available on the chip
ctrlrs total	The total number of HDLC channels on the chip
TDM links	The TDM links connected to the chip
avail DS0s	The number of available DS0s
total DS0s	The total number of DS0s

Related Commands

Command	Description
debug trunk hdlc	Turns on debugging for the HDLC controllers.



show vdev through show voice statistics memory-usage

- show vdev, on page 825
- show vfc, on page 827
- show vfc cap-list, on page 828
- show vfc default-file, on page 829
- show vfc directory, on page 830
- show vfc version, on page 832
- show video call summary, on page 835
- show voice accounting method, on page 836
- show voice accounting response pending, on page 838
- show voice busyout, on page 839
- show voice cable-status, on page 840
- show voice call, on page 841
- show voice call rate, on page 851
- show voice cause-code, on page 853
- show voice class called-number, on page 855
- show voice class called-number-pool, on page 856
- show voice class e164-pattern-map, on page 858
- show voice class e164-translation, on page 859
- show voice class phone-proxy, on page 861
- show voice class resource-group, on page 863
- show voice class server-group, on page 865
- show voice class sip-options-keepalive, on page 867
- show voice class sip-predefined-profiles, on page 868
- show voice class uri, on page 869
- show voice connectivity summary, on page 872
- show voice data, on page 873
- show voice dnis-map, on page 875
- show voice dsmp stream, on page 877
- show voice dsp, on page 884
- show voice dsp channel, on page 892
- show voice dsp crash-dump, on page 895

- show voice dsp summary, on page 897
- show voice eddri prefix, on page 899
- show voice emergency locations, on page 900
- show voice enum-match-table, on page 901
- show voice hpi capture, on page 902
- show voice iec description, on page 903
- show voice lmr, on page 904
- show voice pcm capture, on page 909
- show voice port, on page 910
- show voice sip license, on page 922
- show voice source-group, on page 957
- show voice statistics csr interval accounting, on page 960
- show voice statistics csr interval aggregation, on page 962
- show voice statistics csr since-reset accounting, on page 967
- show voice statistics csr since-reset aggregation-level, on page 969
- show voice statistics csr since-reset all, on page 974
- show voice statistics iec, on page 978
- show voice statistics interval-tag, on page 980
- show voice statistics memory-usage, on page 982

show vdev

To display information about the digital signal processors (DSPs) on a specific card, use the show vdev command in privileged EXEC mode.

show vdev {*slot*/*port*}

Syntax Description

slot	Slot in which the voice card resides.
port	Port on the voice card.

Command Default

No default behavior or values.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.3(2)T	This command was introduced on the Cisco AS5850.

Usage Guidelines

This command can be used on the standby and active route switch controller (RSC) to verify that dynamic and bulk synchronization have been performed correctly on a specified port.

Examples

The following example shows the output for the last port on a 324 universal port card.

```
Router# show vdev 2/323
flags = 0x0000
dev_status = 0x0000
service = 0x0000
service_type = 0x0
min_speed = 0, max_speed = 0
modulation = 0, err_correction = 0, compression = 0
csm_call_info = 0x0, csm_session = Invalid
vdev_p set to modem_info
DSPLIB information:
dsplib_state = 0x0
dsplib_next_action = 0x0
HDLC information:
call_id = 0x0
called_number =
speed = 0
ces = 0x0
spc = FALSE
d_idb = 0x0
Bulk sync reference = 2, Global bulk syncs = 2
```

The table below displays significant fields shown in the output.

Table 167: show vdev Field Descriptions

Field	Description
flags	Internal vdev flags
dev_status	Additional flags giving status of the resource
service	Service currently running on this DSP
service_type	Service type as passed in by RPM
min_speed	Minimum configured modem speed
max_speed	Maximum configured modem speed
modulation	Maximum modulation to be negotiated
err_correction	Error correction to be negotiated
compression	Compression to be negotiated
csm_call_info	Address of the associated csm_call_info structure
csm_session	Session ID as maintained by CSM
vdev_p	Address of the associated resource structure
dsplib_state	State of the resource as seen by the DSPLIB
dsplib_next_action	Next DSPLIB action that should be taken on this resource
call_id	Call identifier if this resource has a HDLC call
called_number	Called number if this resource has a HDLC call
speed	Speed of the connection if this resource has a HDLC call
ces	Circuit emulation service information
spc	True if semi permanent call link
d_idb	Address of the associated D channel idb, if this resource has a HDLC call
Bulk sync reference	Number of times that this resource has been bulk synchronized
Global bulk syncs	Number of bulk synchronizations that the VDEV High Availability client has performed

Related Commands

Command	Description
debug vdev	Turns on debugging for voice devices.
show redundancy	Displays current or historical status and related information on a redundant RSC.

show vfc

To see the entries in the host-name-and-address cache, use the **show vfc**command in privileged EXEC mode.

show vfc *slot-number* [**technology**]

Syntax Description

slot -number	VFC slot number.
technology	(Optional) Displays the technology type of the VFC.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
11.3 NA	This command was introduced on the Cisco AS5300.
12.0(2)XH	The **technology** keyword was added.

Examples

The following is sample output from this command showing that the card in slot 1 is a C549 DSPM:

```
Router# show vfc 1 technology
Technology in VFC slot 1 is C549
```

Field descriptions should be self-explanatory.

Related Commands

Command	Description
voice-card	Configures a voice card and enters voice-card configuration mode.

show vfc cap-list

To show the current list of files on the capability list for this voice feature card (VFC), use the **show vfc cap-list**command in user EXEC mode.

show vfc *slot* **cap-list**

Syntax Description

slot	Slot where the VFC is installed. Range is from 0 to 2.

Command Modes

User EXEC (>)

Command History

Release	Modification
11.3 NA	This command was introduced on the Cisco AS5300.

Examples

The following is sample output from this command:

```
Router# show vfc 1 cap-list
Capability List for VFC in slot 1:
1. fax-vfc-l.0.1.bin
2. bas-vfc-l.0.1.bin
3. cdc-g729-l.0.1.bin
4. cdc-g711-l.0.1.bin
5. cdc-g726-l.0.1.bin
6. cdc-g728-l.0.1.bin
7. cdc-gsmfr-l.0.1.bin
```

The first line in this output is a general description, stating that this is the capability list for the VFC residing in slot 1. Below this is a numbered list, each line of which identifies one currently installed in-service file.

Related Commands

Command	Description
show vfc default -file	Displays the default files included in the default file list for this VFC.
show vfc directory	Displays the list of all files residing on this VFC.
show vfc version	Displays the version of the software residing on this VFC.

show vfc default-file

To show the default files included in the default file list for a voice feature card (VFC), use the **show vfc default-file**command in user EXEC mode.

show vfc *slot* **default-file**

Syntax Description

slot	Slot where the VFC is installed. Range is from 0 to 2.

Command Modes

User EXEC (>)

Command History

Release	Modification
11.3 NA	This command was introduced on the Cisco AS5300.

Examples

The following is sample output from this command:

```
Router# show vfc 1 default-file
Default List for VFC in slot 1:
1. btl-vfc-1.0.13.0.bin
2. cor-vfc-1.0.1.bin
3. bas-vfc-1.0.1.bin
4. cdc-g729-1.0.1.bin
5. fax-vfc-1.0.1.bin
6. jbc-vfc-1.0.13.0.bin
```

The first line in this output is a general description, stating that this is the default list for the VFC residing in slot 1. Below this is a numbered list, each line of which identifies one default file.

Related Commands

Command	Description
show vfc cap -list	Displays the current list of files on the capability list for this VFC.
show vfc directory	Displays the list of all files residing on this VFC.
show vfc version	Displays the version of the software residing on this VFC.

show vfc directory

To show the list of all files residing on a voice feature card (VFC), use the **show vfc directory**command in user EXEC mode.

show vfc *slot* **directory**

Syntax Description

slot	Slot where the VFC is installed. Range is from 0 to 2.

Command Modes

User EXEC (>)

Command History

Release	Modification
11.3 NA	This command was introduced on the Cisco AS5300.

Usage Guidelines

Use this command to display a list of all of the files currently stored in Flash memory for a particular VFC.

Examples

The following is sample output from this command:

```
Router# show vfc 1 directory
Files in slot 1  VFC flash:
     File Name                        Size (Bytes)
1 .  vcw-vfc-mz.gsm.VCW               292628
2 .  btl-vfc-1.0.13.0.bin             4174
3 .  cor-vfc-1.0.1.bin                54560
4 .  jbc-vfc-1.0.13.0.bin             16760
5 .  fax-vfc-1.0.1.bin                64290
6 .  bas-vfc-1.0.1.bin                54452
7 .  cdc-g711-1.0.1.bin               190
8 .  cdc-g729-1.0.1.bin               21002
9 .  cdc-g726-1.0.1.bin               190
10.  cdc-g728-1.0.1.bin               22270
11.  cdc-gsmfr-1.0.1.bin              190
```

The table below describes significant fields in this output.

Table 168: show vfc directory Field Descriptions

Field	Description
File Name	Name of the file stored in Flash memory.
Size (Bytes)	Size of the file in bytes.

Related Commands

Command	Description
show vfc cap -list	Displays the current list of files on the capability list for this VFC.
show vfc default -file	Displays the default files included in the default file list for this VFC.

Command	Description
show vfc version	Displays the version of the software residing on this VFC.

show vfc version

To show the version of the software residing on a voice feature card (VFC), use the **show vfc version**command in user EXEC mode.

show vfc *slot* **version** {**dspware** | **vcware**}

Syntax Description

slot	Slot where the VFC is installed. Range is from 0 to 2.
dspware	Which DSPWare software to display.
vcware	Which VCWare software to display.

Command Modes

Privileged EXEC (#)
User EXEC (>)

Command History

Release	Modification
11.3 NA	This command was introduced on the Cisco AS5300.
12.2(11)T	This command was integrated into Cisco IOS Release 12.2(11)T with changes to the command output.

Usage Guidelines

Use this command to display the version of the software currently installed in Flash memory on a VFC.

Examples

The following is sample output from this command:

```
Router# show vfc 0 version dspware
Version of Dspware in VFC slot 0 is 0.10
```

The output from this command is a simple declarative sentence stating the version number for the selected type of software (in this example, DSPWare) for the VFC residing in the selected slot number (in this example, slot 0).

Cisco IOS Release 12.2(13)T adds new information to the output of the show vfc slot version vcware and show vfc slot version dspware commands. Messages are output if the Cisco VCWare or DSPWare is not compatible with the Cisco IOS image. The new information is advisory only, so there is no action taken if the software is compatible or incompatible.

If the versions detected fall within the defined criteria and are compatible, nothing is output at bootup time. A confirmation line is output when the show vfc version vcware and show vfc version dspware commands are used:

```
Router# show vfc 1 version vcware
Voice Feature Card in Slot 1:
VCWare Version     : 7.35
ROM Monitor Version: 1.3
     DSPWare Version    : 3.4.46L
     Technology         : C549
VCWare/DSPWare version compatibility OK
```

The table below shows output field descriptions for the show vfc version vcware command with compatible firmware.

Table 169: show vfc version vcware Field Descriptions

Field	Description
Voice Feature Card in Slot	Slot in which the VFC is installed.
VCWare Version	Cisco VCWare version. Version 7.35 is the required minimum for Cisco IOS Release 12.2(11)T and higher.
ROM	ROM monitor version shows 1.3 .
DSPWare Version	The DSPWare version shows 3.4.46L, which is the required minimum for Cisco IOS Release 12.2(11)T and higher .
Technology	The technology shows C549. C549 technology is available to support either medium-complexity codecs or high-complexity codecs.
VCWare/DSPWare version compatibility	The Cisco VCWare and DSPWare versions are compatible with Cisco IOS software . Cisco VCWare/DSPWare version compatibility is either OK or shows a mismatch. **Note** This option is available only with Cisco IOS Release 12.2(10) mainline and later release or Cisco IOS Release 12.2(11)T and later.

The following is sample outpou from this command.

```
Router# show vfc 1 version dspware
DSPWare version in VFC slot 1 is 3.4.46L
VCWare/DSPWare version compatibility OK
```

The table below shows output field descriptions for the show vfc version dspware command with compatible firmware.

Table 170: show vfc version dspware Field Descriptions

Field	Description
Voice Feature Card in Slot	Slot in which the VFC is installed .
DSPWare Version	The DSPWare version shows 3.4.46L, which is the required minimum for Cisco IOS Release 12.2(10)T and higher .
VCWare/DSPWare version compatibility	The Cisco VCWare and DSPWare versions are compatible with Cisco IOS software. Cisco VCWare/DSPWare version compatibility is either OK or shows a mismatch. **Note** This option is available only with Cisco IOS Release 12.2(10) mainline and later or 12.2(11)T and later.

If the found versions are out of range or otherwise mismatched, a representative message is output when you boot up the router or is appended to the output of the show vfc version vcware and show vfc version dspware commands. Other than the output of these messages, the version check has no other effect, and the software functions normally. The following is an example of when a found version is out of range or mismatched at bootup :

```
...
Firmware version mismatch for bundle AS5300 VCWare
  -  version found (6.04) is lower than minimum required (7.35)
Firmware version mismatch for bundle AS5300 C549
  - version found (3.3.10L) is lower than minimum required (3.4.46L)
```

If you were to enter an explicit request, and the software were incompatible, the following output would be displayed :

```
Router# show vfc 1 version vcware
Voice Feature Card in Slot 1:
VCWare Version     : 6.04
ROM Monitor Version: 1.3
     DSPWare Version    : 3.3.10L
     Technology         : C549
Firmware version mismatch for bundle AS5300 VCWare
  - version found (6.04) is lower than minimum required (7.14)
Firmware version mismatch for bundle AS5300 C549
  - version found (3.3.10L) is lower than minimum required (3.4.26L)
Router# show vfc 1 version dspware
DSPWare version in VFC slot 1 is 3.3.10L
Firmware version mismatch for bundle AS5300 VCWare
  - version found (6.04) is lower than minimum required (7.14)
Firmware version mismatch for bundle AS5300 C549
  - version found (3.3.10L) is lower than minimum required (3.4.26L)
```

Related Commands

Command	Description
show vfc cap -list	Displays the current list of files on the capability list for this VFC.
show vfc default -file	Displays the default files included in the default file list for this VFC.
show vfc directory	Displays the list of all files residing on this VFC.

show video call summary

To display summary information about video calls and the current status of the Video CallManager (ViCM), use the **show video call summary**command in privileged EXEC mode.

show video call summary

Syntax Description

There are no arguments or keywords.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.0(5)XK	This command was introduced on the Cisco MC3810.
12.0(7)T	The command was integrated into Cisco IOS Release 12.0(7)T.

Usage Guidelines

Use this command to quickly examine the status of current video calls. In Cisco IOS Release 12.0(5)XK and Release 12.0(7)T, there can be only one video call in progress.

Examples

The following example displays information about the ViCM when no call is in progress on the serial interface that connects to the local video codec:

```
Router# show video call summary
Serial0:ViCM =
Idle, Codec Ready
```

The following output shows a call starting:

```
Router# show video call summary
Serial0:ViCM = Call Connected
```

The following output shows a call disconnecting:

```
Router# show video call summary
Serial0:ViCM = Idle
```

Related Commands

Command	Description
show call history video record	Displays information about video calls.

show voice accounting method

To display connectivity status information for accounting method lists, use the **show voice accounting method** command in privileged EXEC mode.

show voice accounting method [*method-list-name*]

Syntax Description

method-list-name	(Optional) Name of a specific method list. This option displays connectivity status information for a single method list identified by this argument.

Command Default

If no argument is specified, connectivity status information for all accounting method lists is displayed.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.3(4)T	This command was introduced.

Usage Guidelines

Use the **show voice accounting method** command to display the history of status (reachable or unreachable), status transition time, and statistics of the accounting status for a specified accounting method list or all the accounting method lists. A maximum of ten status histories are displayed.

Examples

The following is sample output from the **show voice accounting method** command for a specific method list:

```
Router# show voice accounting method ml1
Accounting Method List [ml1]
=======================
Current Status:
---------------
unreachable                [21:52:39 gmt Dec 4 2002]
last record sent time      [23:14:59 gmt Dec 4 2002]
total probe sent out       [84]
Status History:
---------------
(2) unreachable            [21:52:39 gmt Dec 4 2002]
(1) reachable              [21:46:19 gmt Dec 4 2002]
                 SUCCESS                          FAILURE
Record  [Received   | Notified ] [Received   |  Notified  | Reported ]
Type    [from server| to client] [from server|  to client | to call  ]
------  [-----------|----------] [-----------|------------|----------]
START   [     0     |     0    ] [     0     |      0     |     0    ]
UPDATE  [     0     |     0    ] [     0     |      0     |     0    ]
STOP    [     0     |     0    ] [     84    |      84    |     0    ]
ACCT_ON [     0     |     0    ] [     0     |      0     |     0    ]
------  [-----------|----------] [-----------|------------|----------]
TOTAL   [     0     |     0    ] [     84    |      84    |     0    ]
```

If there is no status history, as in the following example, no status history is displayed.

```
Router# show voice accounting method
```

```
Accounting Method List [ml1]
=======================
Current Status:
---------------
reachable                   [21:52:39 gmt Dec 4 2002]
last record sent time       [23:14:59 gmt Dec 4 2002]
total probe sent out        [2]
                SUCCESS                         FAILURE
Record  [Received    | Notified ] [Received    |  Notified  | Reported ]
Type    [from server| to client] [from server|  to client  | to call  ]
------  [-----------|----------] [-----------|------------|----------]
START   [     0      |     0    ] [     0      |      0     |     0    ]
UPDATE  [     0      |     0    ] [     0      |      0     |     0    ]
STOP    [     0      |     0    ] [     2      |      2     |     0    ]
ACCT_ON [     0      |     0    ] [     0      |      0     |     0    ]
------  [-----------|----------] [-----------|------------|----------]
TOTAL   [     0      |     0    ] [     2      |      2     |     0    ]
```

The table below describes the significant fields shown in the display.

Table 171: show voice accounting method Field Descriptions

Field	Description
Current Status: reachable or unreachable	Current status of the method list: reachable or unreachable and the time (in hh:mm:ss) and date the method list reached this status.
last record sent time	Time (in hh:mm:ss) and date the last accounting record was sent to the method list.
total probe sent out	Number of probe records sent up to the time of the show command.
SUCCESS: Received from server	Number of success status of the accounting records of this type received from the method list.
SUCCESS: Notified to client	Number of success status of the accounting records of this type for which notifications were sent to the GAS.
FAILURE: Received from server	Number of failure status of the accounting records of this type received from the method list.
FAILURE: Notified to client	Number of failure status of the accounting records of this type for which notifications were sent to the GAS.
FAILURE: Reported to call	Number of failure status of the accounting records of this type that were reported to the call application.

Related Commands

Command	Description
clear voice accounting method	Clears accounting status statistics for a particular accounting method list or all accounting method lists.

show voice accounting response pending

To display information regarding pending VoIP AAA accounting responses, use the **show voice accounting response pending**command in privileged EXEC mode.

show voice accounting response pending

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.3(4)T	This command was introduced.

Examples

The following example displays information regarding pending VoIP AAA accounting responses:

```
Router# show voice accounting response pending
Total num of acct sessions waiting for acct responses: 0
Total num of acct start responses pending:             0
Total num of acct interim update responses pending:     0
Total num of acct stop responses pending:              0
```

The table below lists and describes the significant output fields.

Table 172: show voice accounting response pending Field Descriptions

Field	Description
Total num of acct sessions waiting for acct responses	Number of accounting sessions that are waiting for accounting responses.
Total num of acct start responses pending	Number of accounting start responses that are pending.
Total num of acct interim update responses pending	Number of accounting interim update responses that are pending.
Total num of acct stop responses pending	Number of accounting stop responses that are pending.

show voice busyout

To display information about the voice-busyout state, use the **show voice busyout** command in privileged EXEC mode.

show voice busyout

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.0(3)T	This command was introduced on the Cisco MC3810.
12.0(7)XK	This command was implemented on the Cisco 2600 series and Cisco 3600 series.
12.1(2)T	This command was integrated into Cisco IOS Release 12.1(2)T.

Usage Guidelines

This command displays the following information:

- Interfaces that are being monitored for busyout events
- Voice ports currently in the busyout state and the reasons

Examples

The following is sample output from this command:

```
Router# show voice busyout
If following network interfaces are down, voice port will be put into busyout state
ATM0
Serial0
The following voice ports are in busyout state
1/1      is forced into busyout state
1/2      is in busyout state caused by network interfaces
1/3      is in busyout state caused by ATM0
1/4      is in busyout state caused by network interfaces
1/5      is in busyout state caused by Serial0
```

Field descriptions should be self-explanatory.

Related Commands

Command	Description
busyout forced	Forces a voice port into the busyout state.
busyout monitor	Places a voice port in the busyout monitor state.
busyout seize	Changes the busyout seize procedure from a voice port.
voice-port busyout	Places all voice ports associated with a serial or ATM interface in a busyout state.

show voice cable-status

To display the current or last cable status of a specific analog voice port or all idle analog voice ports, use the **show voice cable-status** command in privileged EXEC mode.

show voice cable-status {**all** | **summary***x/y/zx/y/z-z1*}

Syntax Description

all	Specifies the current cable status of all analog voice ports that have cable polling enabled.
summary	Specifies the last cable status of all analog voice ports that have cable polling enabled.
x/y/z	Voice port number.
x/y/z-z1	Voice port number range. The range is from 0 to 71. Example: 2/0/0-71.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
15.2(4)M	This command was introduced.

Usage Guidelines

Before using the **show voice cable-status** command, you must disable the **cable-detect-poll-timer** command.

Examples

The following is sample output from the **show voice cable-status all** command:

```
Device# show voice cable-status all

Warning:This may take time to perform and cause call disruption!

PORT         cable-status
========== ================
0/2/0        cable-detect not configured
0/2/1        connected
0/2/2        connected
0/2/3        busy out
0/3/0        administrative down
0/3/1        in busy state
0/3/2        connected
0/3/3        connected
1/0/16       not connected
```

Related Commands

Command	Description
cable-detect	Enables cable polling on analog FXOGS, FXOLS, FXSGS, and FXSLS voice ports.
cable-detect-poll-timer	Configures the cable polling timer value for background polling processes on an analog voice port.

show voice call

To display the call status for voice ports on the Cisco router, use the **show voice call** command in user EXEC or privileged EXEC mode.

Cisco 827, Cisco 1700 Series, and Cisco 7750 with Analog Voice Ports
show voice call [*slot/port* | **status** [*call-id*] [**sample** *seconds*] | **summary**]

Cisco 2600, Cisco 3600, Cisco 3700 Series with Analog Voice Ports
show voice call [*slot/stubunit/port* | **status** [*call-id*] [**sample** *seconds*] | **summary**]

Cisco 2600, Cisco 3600, and Cisco 3700 Series with Digital Voice Ports (with T1 Packet Voice Trunk Network Modules)
show voice call [*slot/port*:*ds0-group* | **status** [*call-id*] [**sample** *seconds*] | **summary**]

Cisco AS5300, Cisco AS5350, Cisco AS5400, Cisco AS5850, Cisco 7200 Series, and Cisco 7500 Series with Digital Voice Ports
show voice call [*slot/port*:*ds0-group* | **status** [*call-id*] [**sample** *seconds*] | **summary**]

Syntax Description

Cisco 827, Cisco 1700 Series, and Cisco 7750 with Analog Voice Ports	
slot /*port*	(Optional) A specific analog voice port: • *slot*-- Physical slot in which the analog voice module (AVM) is installed. • / *port* --Analog voice port number. Range is from 1 to 6. The slash mark is required.
status [*call-id*]	(Optional) Displays status of active calls. If *call-id* is specified, this command displays the status of a specific call .
sample *seconds*	(Optional) Displays status over a specified sampling interval, in seconds. Range is from 1 to 30. Default is 10.
summary	(Optional) Displays current settings and state of the voice port, regardless of port activity.

Cisco 2600 Series, Cisco 3600 Series, Cisco 3700 Series with Analog Voice Ports	
slot / *subunit* / *port*	(Optional) A specific analog voice port: • *slot* --Router slot in which a voice network module (NM) is installed. Valid entries are router slot numbers for the particular platform. • / *subunit* -- Voice interface card (VIC) in which the voice port is located. Valid entries are 0 and 1. (The VIC fits into the voice network module.) The slash mark is required. • / *port* -- Analog voice port number. Valid entries are 0 and 1. The slash mark is required.
status [*call-id*]	(Optional) Displays status of active calls. If *call-id* is specified, this command displays the status of a specific call .
sample *seconds*	(Optional) Displays status over a specified sampling interval, in seconds. Range is from 1 to 30. Default is 10.
summary	(Optional) Displays current settings and state of the voice port, regardless of port activity.

Cisco 2600, Cisco 3600, and Cisco 3700 Series with Digital Voice Ports (with T1 Packet Voice Trunk Network Modules)	
slot / *port* **:** *ds0 -group*	(Optional) A specific digital voice port: • *slot* -- Router slot in which the packet voice trunk network module (NM) is installed. Valid entries are router slot numbers for the particular platform. • / *port* --T1 or E1 physical port in the voice WAN interface card (VWIC). Valid entries are 0 and 1. (One VWIC fits in an NM.) The slash mark is required. • **:** *ds0 -group*--T1 or E1 logical port number. Range is from 0 to 23 for T1 and from 0 to 30 for E1. The colon is required.
status [*call-id*]	(Optional) Displays status of active calls. If *call-id* is specified, this command shows the status of a specific call .
sample *seconds*	(Optional) Displays status over a specified sampling interval, in seconds. Range is from 1 to 30. Default is 10.
summary	(Optional) Displays current settings and state of the DSP port regardless of port activity.

Cisco AS5300, Cisco AS5350, Cisco AS5400, Cisco AS5850, Cisco 7200 Series, and Cisco 7500 Series with Digital Voice Ports	
slot / *port* : *ds0 -group*	(Optional) A specific digital voice port: • *slot* --Router slot in which the packet voice trunk network module (NM) is installed. Valid entries are router slot numbers for the particular platform. • / *port*-- T1 or E1 physical port in the VWIC. Valid entries are 0 and 1. (One VWIC fits in an NM.) The slash mark is required. • : *ds0 -group*--T1 or E1 logical port number. Range is from 0 to 23 for T1 and from 0 to 30 for E1. The colon is required.
status [*call-id*]	(Optional) Displays status of active calls. If *call-id* is specified, this command shows the status of a specific call .
sample *seconds*	(Optional) Displays status over a specified sampling interval, in seconds. Range is from 1 to 30. Default is 10.
summary	(Optional) Displays current settings and state of the voice port regardless of port activity.

Command Modes

User EXEC (#)
privileged EXEC (>)

Command History

Release	Modification
11.3(1)MA	This command was introduced on the Cisco MC3810.
12.0(7)XK	This command was implemented on the Cisco 2600 series and Cisco 3600 series.
12.1(2)T	This command was integrated into Cisco IOS Release 12.1(2)T.
12.2(13)T	This command was modified with the **status**, *call-id*, and **sample** *seconds* command options. This command is available on all voice platforms.
12.4(3d)	This command was modified to support the Cisco AS5350, Cisco AS5400, and Cisco AS5850 platforms for Non-Facility Associated Signaling (NFAS) configuration. Output was modified to provide accurate port information for NFAS configuration on these platforms.
15.1(3)T	This command was modified. The output of this command was enhanced to display the connection status of foreign exchange office (FXO) ports.

Usage Guidelines

This command works on Voice over Frame Relay, Voice over ATM, and Voice over IP by providing the status at the following levels of the call-handling module:

- Call-processing state machine

- End-to-end call manager
- Protocol state machine
- Tandem switch

Note This command is not supported in Cisco AS5350, Cisco AS5400, and Cisco AS5850 platforms for NFAS configuration before Cisco IOS Release 12.4(3d).

This command displays call-processing and protocol state-machine information for a voice port if the information is available. This command also shows information on the DSP channel associated with the voice port if the information is available. All real-time information in the DSP channel, such as jitter and buffer overrun, is queried to the DSP channel, and asynchronous responses are returned to the host side.

If no call is active on a voice port, the **show voice call summary** command displays only the VPM (shutdown) state. If a call is active on a voice port, the **show voice call summary** command displays voice telephony service provider (VTSP) state. For an on-net call or a local call without local bypass (not cross-connected), the codec and voice activity detection (VAD) fields are displayed. For an off-net call or a local call with local bypass, the codec and VAD fields are not displayed.

When a call is active on a voice port, the **show voice call summary** command displays the VTSP state. The VTSP state always shows the VTSP signaling state irrespective of the type of call: voice call or a fax call. A fax call does not display S_Fax. The following output is displayed:

```
PORT            CODEC    VAD VTSP STATE             VPM STATE
=============== ======== === ==================== ======================
1/0:1.1          1         y  S_CONNECT             EM_CONNECT
```

Note Use the **show voice dsmp stream** command to display the current session of the voice Distributed Stream Media Processor (DSMP) media stream and its related applications.

The **show voice call** command does not display the codec and VAD fields because this information is in the summary display. If you use the **show voice call status**command by itself, an immediate list of all the active calls is shown. You can use the *call-id* argument to request that the DSP associated with the *call-id* be queried for run-time statistics twice, once immediately, and a second time after **sample** *seconds*.

The **sample** *seconds* is the number of seconds over which the status is to be determined. The results of the run-time statistic queries are then analyzed and presented in a one-line summary format.

When a call terminates during the specified sample period , the following output message is returned:

```
CallID call id cannot be queried
CallID call id second sample responses unavailable
```

Note The Voice Call Tuning feature is not supported on the Cisco AS5300.

Examples

The following is sample output from the **show voice call summary** command showing two local calls connected without local bypass:

```
Router# show voice call summary
PORT    CODEC    VAD VTSP STATE              VPM STATE
======= ======== === ===================== ========================
0:17.18                                      *shutdown*
0:18.19 g729ar8   n  S_CONNECT              FXOLS_OFFHOOK
0:19.20                                      FXOLS_ONHOOK
0:20.21                                      FXOLS_ONHOOK
0:21.22                                      FXOLS_ONHOOK
0:22.23                                      FXOLS_ONHOOK
0:23.24                                      EM_ONHOOK
1/1                                          FXSLS_ONHOOK
1/2                                          FXSLS_ONHOOK
1/3                                          EM_ONHOOK
1/4                                          EM_ONHOOK
1/5                                          FXOLS_ONHOOK
1/6     g729ar8   n  S_CONNECT              FXOLS_CONNECT
```

The following is sample output from the **show voice call summary** command showing two local calls connected with local bypass:

```
Router# show voice call summary
PORT    CODEC    VAD VTSP STATE              VPM STATE
======= ======== === ===================== ========================
0:17.18                                      *shutdown*
0:18.19              S_CONNECT              FXOLS_OFFHOOK
0:19.20                                      FXOLS_ONHOOK
0:20.21                                      FXOLS_ONHOOK
0:21.22                                      FXOLS_ONHOOK
0:22.23                                      FXOLS_ONHOOK
0:23.24                                      EM_ONHOOK
1/1                                          FXSLS_ONHOOK
1/2                                          FXSLS_ONHOOK
1/3                                          EM_ONHOOK
1/4                                          EM_ONHOOK
1/5                                          FXOLS_ONHOOK
1/6                  S_CONNECT              FXOLS_CONNECT
```

The following is sample output from the **show voice call summary** command in which the connected FXO port 0/2/0 shows status of "FXOLS_ONHOOK" whereas the FXO port 0/2/1, which is disconnected, shows a status of "FXOLS_BUSYOUT":

```
Router# show voice call summary
PORT           CODEC     VAD VTSP STATE             VPM STATE
============== ========= === =================== ======================
0/0/0          -           -  -                    FXSLS_ONHOOK
0/0/1          -           -  -                    FXSLS_ONHOOK
0/3/0:23.1       -           -  -
0/3/0:23.2       -           -  -
.
.
.
0/3/0:23.23      -           -  -
0/1/0          -           -  -                    DID_ONHOOK
0/1/1          -           -  -                    DID_ONHOOK
0/2/0          -           -  -                    FXOLS_ONHOOK
0/2/1          -           -  -                    FXOLS_BUSYOUT
2/0/0          -           -  -                    FXSLS_ONHOOK
2/0/1          -           -  -                    FXSLS_ONHOOK
```

```
2/0/2          -          -  -                    FXSLS_ONHOOK
2/0/3          -          -  -                    FXSLS_ONHOOK
2/0/4          -          -  -                    FXSLS_ONHOOK
2/0/5          -          -  -                    FXSLS_ONHOOK
2/0/6          -          -  -                    FXSLS_ONHOOK
2/0/7          -          -  -                    FXSLS_ONHOOK
```



Note Beginning in Cisco IOS Release 15.1(3)T, there is improved status monitoring of FXO ports--any time an FXO port is connected or disconnected, a message is displayed to indicate the status change. For example, the following message is displayed to report that a cable has been connected, and the status is changed to "up" for FXO port 0/2/0: 000118: Jul 14 18:06:05.122 EST: %LINK-3-UPDOWN: Interface Foreign Exchange Office 0/2/0, changed state to operational status up due to cable reconnection

The following is sample output from the **show voice call summary** command showing one regular PRI port and one NFAS PRI port on a Cisco AS5350, Cisco AS5400, or Cisco AS5850 platform. Port 3/2:D belongs to a regular PRI voice port with time slots 0 and 22. Port Se3/1 belongs to an NFAS PRI voice port with time slots 0,1, and 2 on T1 controller 3/1, which is a member of an NFAS group.

In the case of NFAS on Cisco AS5350, Cisco AS5400, and Cisco AS5850 platforms, the port is reported in terms of the serial interface associated with the T1 controller, and the time slot is counted from 0 (for example, 0, 1, 2, 3).

```
Router# show voice call summary
PORT           CODEC    VAD VTSP STATE             VPM STATE
============== ======== === ==================== ======================
3/2:D.0        None      y  S_ALERTING            S_TSP_INCALL
3/2:D.22       None      y  S_ALERTING            S_TSP_INCALL
Se3/1:0        None      y  S_CONNECT             S_TSP_CONNECT
Se3/1:1        None      y  S_CONNECT             S_TSP_CONNECT
Se3/1:2        None      y  S_CONNECT             S_TSP_CONNECT
```



Note The output from the **show voice call summary** command is slightly different in the PORT field on platforms other than the Cisco AS5350, Cisco AS5400, and Cisco AS5850. The contrast between platform types is as follows: Platform Regular PRI (T1) NFAS PRI (T1)* ---------- non-AS5xxx 3/0:23.TS 3/1:23.TS AS5xxx 3/0:D.TS Ser3/1:(TS-1) * Assumes T1 3/1 is a member of an NFAS group with T1 3/0 as the primary NFAS member, and TS is the time slot counted from a base of 1 (for example 1, 2, 3).

The following is sample output from the **show voice call** command for analog voice ports:

```
Router# show voice call
1/1 vpm level 1 state = FXSLS_ONHOOK
vpm level 0 state = S_UP
1/2 vpm level 1 state = FXSLS_ONHOOK
vpm level 0 state = S_UP
1/3 is shutdown
1/4 vtsp level 0 state = S_CONNECT
vpm level 1 state = S_TRUNKED
```

```
vpm level 0 state = S_UP
1/5 vpm level 1 state = EM_ONHOOK
vpm level 0 state = S_UP
1/6 vpm level 1 state = EM_ONHOOK
vpm level 0 state = S_UP
Router# show voice call 1/4
1/4 vtsp level 0 state = S_CONNECT
vpm level 1 state = S_TRUNKED
vpm level 0 state = S_UP
router#   ***DSP VOICE VP_DELAY STATISTICS***
Clk Offset(ms): 1445779863, Rx Delay Est(ms): 95
Rx Delay Lo Water Mark(ms): 95, Rx Delay Hi Water Mark(ms): 125
  ***DSP VOICE VP_ERROR STATISTICS***
Predict Conceal(ms): 10, Interpolate Conceal(ms): 0
Silence Conceal(ms): 0, Retroact Mem Update(ms): 0
Buf Overflow Discard(ms): 20, Talkspurt Endpoint Detect Err: 0
  ***DSP VOICE RX STATISTICS***
Rx Vox/Fax Pkts: 537, Rx Signal Pkts: 0, Rx Comfort Pkts: 0
Rx Dur(ms): 50304730, Rx Vox Dur(ms): 16090, Rx Fax Dur(ms): 0
Rx Non-seq Pkts: 0, Rx Bad Hdr Pkts: 0
Rx Early Pkts: 0, Rx Late Pkts: 0
  ***DSP VOICE TX STATISTICS***
Tx Vox/Fax Pkts: 567, Tx Sig Pkts: 0, Tx Comfort Pkts: 0
Tx Dur(ms): 50304730, Tx Vox Dur(ms): 17010, Tx Fax Dur(ms): 0
  ***DSP VOICE ERROR STATISTICS***
Rx Pkt Drops(Invalid Header): 0, Tx Pkt Drops(HPI SAM Overflow): 0
  ***DSP LEVELS***
TDM Bus Levels(dBm0): Rx -70.3 from PBX/Phone, Tx -68.0 to PBX/Phone
TDM ACOM Levels(dBm0): +2.0, TDM ERL Level(dBm0): +5.6
TDM Bgd Levels(dBm0): -71.4, with activity being voice
```

The following is sample output from the **show voice call** command for analog voice ports on a Cisco 7200 series. The output includes the DSPfarm, T1 interface, and DS0 or TLM slot configuration:

```
Router# show voice call 6/0:0
6/0:0 1 -         -  -                    vpm level 1 state = FXOGS_ONHOOK
vpm level 0 state = S_UP
6/0:0 2 -         -  -                    vpm level 1 state = FXOGS_ONHOOK
vpm level 0 state = S_UP
6/0:0 3 -         -  -                    vpm level 1 state = FXOGS_ONHOOK
vpm level 0 state = S_UP
6/0:0 4 -         -  -                    vpm level 1 state = FXOGS_ONHOOK
vpm level 0 state = S_UP
6/0:0 5 -         -  -                    vpm level 1 state = FXOGS_ONHOOK
vpm level 0 state = S_UP
6/0:0 6 -         -  -                    vpm level 1 state = FXOGS_ONHOOK
vpm level 0 state = S_UP
6/0:0 7 -         -  -                    vpm level 1 state = FXOGS_ONHOOK
vpm level 0 state = S_UP
6/0:0 8 -         -  -                    vpm level 1 state = FXOGS_ONHOOK
vpm level 0 state = S_UP
6/0:0 9 -         -  -                    vpm level 1 state = FXOGS_ONHOOK
vpm level 0 state = S_UP
6/0:0 10-         -  -                    vpm level 1 state = FXOGS_ONHOOK
vpm level 0 state = S_UP
6/0:0 11-         -  -                    vpm level 1 state = FXOGS_ONHOOK
vpm level 0 state = S_UP
6/0:0 12-         -  -                    vpm level 1 state = FXOGS_ONHOOK
vpm level 0 state = S_UP
```

The following is sample output from the **show voice call status**command on the Cisco 2600 series. You can use this command rather than the **show call active brief**command to obtain the caller ID; the caller ID output of the **show voice call status**command is already in hexadecimal form.

```
Router# show voice call status
CallID     CID  ccVdb      Port      DSP/Ch  Called #   Codec    Dial-peers
0x1        11CE 0x02407B20 1:0.1     1/1     1000       g711ulaw 2000/1000
1 active call found
```

Using the *call-id* argument is a generic means to identify active calls. If the *call-id* is omitted, the query shows all active voice calls. In the following example, a list of all active calls with relevant identifying information is shown:

```
Router# show voice call status
CallID    CID    ccVdb       Port     DSP/Ch  Called #   Codec    Dial-peers
0x3       11D4   0x62972834  1/0/0    1/1     10001      g711ulaw 1/2
0x4       11D4   0x62973AD0  1/0/1    2/1    *10001      g711ulaw 2/1
0xA       11DB   0x62FE9D68  1/1/0    3/1    *2692       g729r8   0/2692
2 active calls found
```

Note You can query only one call at a time. If you attempt queries from different ports (console and Telnet), and if a query is in progress on another port, the system asks you to wait for completion of that query. You can query any call from anywhere, at anytime, except during the sample interval for an enquiry that is already in progress. This simplifies the implementation significantly and does not reduce the usefulness of the command.

The following example shows echo-return-loss (ERL) reflector information where the call ID is 3 and the sample period is 10 seconds:

```
Router# show voice call status 3 sample 10
Gathering information (10 seconds)...
CallID    Port     DSP/Ch  Codec    Rx/Tx     ERL         Jitter
0x3       1/0/0    1/1     g711ulaw 742/154   5.6         50/15
```

In this example, ERL is the echo return loss (in dB) as reported by the DSP. Jitter values are the current delay and the jitter of the packets around that delay.

If the router is running the extended echo canceller, output looks similar to the following if you enter the same command. The output shows a new value under ERL/Reflctr: the time difference, in ms, between the original signal and the loudest echo (peak reflector) as detected by the echo canceller:

```
Router# show voice call status 3 sample 10
Gathering information (10 seconds)...
CallID    Port     DSP/Ch  Codec    Rx/Tx     ERL/Reflctr Jitter
0x3       1/0/0    1/1     g711ulaw 742/154   5.6/12      50/15
```

The following examples show output using the NextPort version of the standard echo canceller. (Time-slot information is also in the output for digital ports.)

```
Router# show voice call status
CallID     CID  ccVdb      Port      DSP/Ch  Called #   Codec    Dial-peers
0x97       12BB 0x641B0F68 3/0:D.1   1012/2  31001      g711ulaw 3/31000
0x99       12BE 0x641B0F68 3/0:D.2   1012/3  31002      g711ulaw 3/31000
2 active calls found
Router# show voice call status
CallID     CID  ccVdb       Port     DSP/Ch  Called #   Codec    Dial-peers
0x2        11D1 0x62FE6478 1/0/0     1/1     10001      g711ulaw 1/2
0x3        11D1 0x62FE80F0 1/0/1     2/1    *10001      g711ulaw 2/1
1 active call found
```

When using the **test call id** command, you must specify a call ID, which you can obtain by using the **show voice call status** command. The following is an example of how to obtain the call ID for use as the *call-id* argument. The first parameter displayed in the output is the call ID.

Note Do not use the 0x prefix in the *call-id* argument when you enter the resulting call ID in the **test call status**command .

The following shows keyword choices when using the **show voice call** command with the | (pipe) option:

```
Router# show voice call | ?
  append    Append redirected output to URL (URLs supporting append operation
            only)
  begin     Begin with the line that matches
  exclude   Exclude lines that match
  include   Include lines that match
  redirect  Redirect output to a URL
  tee       Copy output to a URL
```

The table below describes significant fields shown in the previous displays.

Table 173: show voice call Field Descriptions

Field (listed alphabetically)	Description
Called #	Called number. • No "*" before the number denotes an originating call leg. Two of the call legs in the example constitute one locally switched call and one network call, so the call legs refer to two active calls. • A "*" before the number denotes a destination call leg (for example, this number was called with Called #).
CallID	This hexadecimal number used for further query is the monotonically increasing number that call control maintains for each call leg (ccCallID_t).
ccVdb	Value that is displayed in many other debugs to identify these call legs.
CID	Conglomerate value derived from the GUID that appears in the **show call active brief**command.
Codec	Codec.
Dial-peers	Dial peer .
DSP/Ch	DSP and channel allocated to this call leg. The format of these values is platform dependent (particularly the Cisco AS5300, which shows the DSP number as a 3-digit number, <VFC#><DSPM#><DSP#>). Time-slot information is also in the output for digital ports. For example, if you are using a digital port, the time slot is also returned: dsp/ch/ time slot .
ERL	Echo return loss (in dB).

Field (listed alphabetically)	Description
ERL/Reflctr	Time difference, in ms, between the original signal and the loudest echo (peak reflector) as detected by the echo canceller.
Jitter	Current values of the delay and the jitter of the packets around that delay.
Port	V oice port.
Rx/Tx	Transmit and receive rates for the connection.
VAD	Voice-activity detection: y or n.
VPM STATE	Voice-port-module (VPM) state.
VTSP STATE	Voice-telephony-service-provider (VTSP) state.

For more information about the extended echo canceller, see *Extended ITU-T G.168 Echo Cancellation*
.

Related Commands

Command	Description
show call active brief	Displays a summary of active call information.
show dial-peer voice	Displays the configuration for all VoIP and POTS dial peers configured on the router.
show voice dsmp stream	Displays the current session of the voice DSPM media stream.
show voice dsp	Displays the current status of all DSP voice channels.
show voice port	Displays configuration information about a specific voice port.
test call id	Manipulates the echo canceller and jitter buffer parameters in real time.

show voice call rate

Note With CSCuc53349, the **show voice call rate** command is replaced by the **show call history stats cps**command. See the **show call history stats cps** command for more information.

To display the voice call rate information, use the **show voice call rate** command in privileged EXEC mode.

show voice call rate [**table**]

Syntax Description

table	(Optional) Displays the voice call rate information in a tabular format.

Command Default

Displays the voice call rate information in a histogram format.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
15.2(2)T	This command was introduced.
15.3(2)T	This command was replaced by the **show call history stats cps** command.
Cisco IOS XE Release 3.9S	This command was replaced by the **show call history stats cps** command.

Usage Guidelines

You can use the **show voice call rate** command to display the voice call rate information in the histogram format. Use the **show voice call rate table** command to display the voice call rate information in a tabular format.

Examples

The following is sample output from the **show voice call rate** command. In the output, x-axis measures time in seconds (1 unit = 1 second) and y-axis measures call legs per second (cps) (1 unit = 1 cps):

```
Router# show voice call rate

3845-1   04:35:57 AM Wednesday Sep 7 2011 UTC
          122                    11
          5009          2        40      42    64
  100
   90
   80
   70
   60
   50
   40
   30
   20    ***
   10    ****                     **              *
     0....5....1....1....2....2....3....3....4....4....5....5....6
                  0    5    0    5    0    5    0    5    0    5    0
```

```
          VoIP Call switching rate per second (last 60 seconds)
          # = calls entering the module per second
```

The following is sample output from the **show voice call rate table** command:

```
Router# show voice call rate table

3845-1   04:35:57 AM Wednesday Sep 7 2011 UTC
          Voice Call switching rate per second (last 60 seconds)
Period     Actual     Average
-------------------------------------
 1-5            0          0
 6-10          64         13
11-15           0          0
16-20           0          0
21-25           2          0
26-30           0          0
31-35          24          5
36-40           0          0
41-45           6          1
46-50          10          2
51-55           0          0
56-60           0          0
```

The following table describes the significant fields shown in the display.

Table 174: show voice call rate table Field Descriptions

Field	Description
Period	Duration of 5 seconds.
Actual	Number of call legs created in 5 seconds.
Average	The average call legs created in 5 seconds.

Related Commands

Command	Description
voice call rate monitoring	Enables voice call rate monitoring.

show voice cause-code

To display error category to Q.850 cause code mapping, use the show voice cause-code command in user EXEC mode.

show voice cause-code category-q850

Syntax Description

category q850	Displays error category to Q.850 cause code mapping.

Command Default

No default behavior or values.

Command Modes

User EXEC (>)

Command History

Release	Modification
12.3(4)T	This command was introduced.

Usage Guidelines

Use this command to display the internal error category to Q.850 cause code mapping table, and configured and default values, with category descriptions.

Examples

The following example displays Q.850 cause code mapping:

```
Router# show voice cause-code category-q850
The Internal Error Category to Q850 cause code mapping table:-
 Error Configured Default    Description
Category  Q850     Q850
   128     27        3  Destination address resolution failure
   129     38      102  Call setup timeout
   178     41       41  Internal Communication Error
   179     41       41  External communication Error
   180     47       47  Software Error
   181     47       47  Software Resources Unavailable
   182     47       47  Hardware Resources Unavailable
   183     41       41  Capability Exchange Failure
   184     49       49  QoS Error
   185     41       41  RTP/RTCP receive timer expired or bearer layer failure
   186     38       38  Signaling socket failure
   187     38       38  Gateway or signaling interface taken out of service
   228     50       50  User is denied access to this service
   278     65       65  Media Negotiation Failure due to non-existing Codec
```

The table below describes the significant fields shown in the display.

Table 175: show voice cause-code Field Descriptions

Field	Description
128	Destination address resolution failure
129	Call setup timeout

Field	Description
178	Internal communication error
179	External communication Error
180	Software error
181	Software resources unavailable
182	Hardware resources unavailable
183	Capability exchange failure
184	QoS error
185	RTP/RTCP receive timer expired or bearer layer failure
186	Signaling socket failure
187	Gateway or signaling interface taken out of service
228	User denied access to this service
278	Media negotiation failure due to non existing codec

Related Commands

Command	Description
error-category q850-cause	Specifies Q.850 cause code mapping

show voice class called-number

To display a specific voice class called-number, use the **show voice class called-number** command in privileged EXEC mode.

show voice class called-number [**inbound** | **outbound**] *tag*

Syntax Description

inbound	Displays the specified inbound voice class called-number.
outbound	Displays the specified outbound voice class called-number.
tag	Digits that identify this voice class called-number.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.4(11)T	This command was introduced.

Usage Guidelines

Use this command to display a specific inbound or outbound voice class called-number.

Examples

The following is sample output from this command:

```
Router# show voice class called-number outbound 200
Called Number Outbound: 200
           index 1      4085550100
           index 2      4085550102
           index 3      4085550103
           index 4      4085550104
```

The table below describes significant fields shown in the display.

Table 176: show voice class called-number Field Descriptions

Field	Description
Called Number Inbound/Outbound	The tag for the specified inbound or outbound voice class called-number.
index *number*	The number or range of numbers for this voice class called number.

Related Commands

Command	Description
show voice class called-number-pool	Displays voice class called number pool configuration information.

show voice class called-number-pool

To display a voice class called-number pool, use the **show voice class called-number-pool** command in privileged EXEC mode.

show voice class called-number-pool tag [**detail**]

Syntax Description

tag	Digits that identify this voice class called-number-pool. Range is 1 to 10000.
detail	Displays idle called number and allocated called number information.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.4(11)T	This command was introduced.

Usage Guidelines

Use this command to display the voice class called number pool configuration information. The **detail** keyword displays up to 16 idle called numbers, and up to 4 allocated called numbers for each allocated request.

Examples

The following sample output displays configuration information for voice class called-number-pool 100, including idle called numbers and allocated called numbers:

```
Router(config)# show voice class called-number-pool 100 detail
Called Number Pool: 100
index 1 100A11 - 100A20
index 2 200#55 - 200#77
index 3 5551111 - 6662333
index 99 123C11 - 123C99
All called numbers are generated from table: FALSE
No of idle called numbers: 16
List of idle called numbers:
100A11 100A12 .. Display up to 16 idle called number from the pool
100A13 100A14
100A15 100A16
100A17 100A18
100A19 100A20
200#55 200#56
200#57 200#58
200#59 200#60
No of alloc requests : 1
Ref Id Alloc PC Size
2 41F84190 16
List of alloc called numbers: .. Display the first 4 allocated called number for RefId 2
200#61 200#62
200#63 200#64
```

The table below describes significant fields shown in the display.

Table 177: show voice class called-number-pool Field Descriptions

Field	Description
Called Number Pool	Tag that identifies the called number pool.
index	Number or range of numbers for this called number pool.
All called numbers are generated from table	• FALSE--Numbers are not generated from called number table. • TRUE--Numbers are generated from called number table.
No. of idle called numbers	Number of idle called numbers in the called number pool.
List of idle called numbers	List of idle numbers in the called number pool.
No. of alloc requests	Number of requests for numbers from the called number pool.
Ref Id Alloc PC Size	Reference ID for a specific list of allocated numbers.
List of alloc called numbers	List of first four allocated numbers from the called number pool.

Related Commands

Command	Description
show voice class called-number	Displays a specific voice class called-number.

show voice class e164-pattern-map

To display the configuration of a voice class E.164 pattern map, use the **show voice class e164-pattern-map** command in user EXEC or privileged EXEC mode.

```
show voice class e164-pattern-map [summary tag]
```

Syntax Description

summary	(Optional) Displays the summary information of the configuration.
tag	(Optional) Displays the status and content of E.164 pattern maps.

Command Modes

User EXEC (>)

Privileged EXEC (#)

Command History

Release	Modification
15.2(4)M	This command was introduced.

Usage Guidelines

You can use the **show voice class e164-pattern-map** command to display the status of a map and all E.164 patterns in the map. This command is used not only to display E.164 patterns in a text file, but E.164 patterns configured through the CLI. But for parsing error, the command applies only to a text file.

Examples

The following is sample output from the **show voice class e164-pattern map** command:

```
Device# show voice class e164-pattern-map summary

e164-pattern-map 1
----------------------------------------
It has 100 entries
It is populated from url http://http-host/config-files/destination-pattern-map.cfg

e164-pattern-map 2
----------------------------------------
It has 23 entries

e164-pattern-map 3
----------------------------------------
Loading failed on url http://http-host/config-files/destination-pattern-map-1.cfg

e164-pattern-map 4
----------------------------------------
Parsing error on patterns: "123gh" "1*g"
It is populated from url http://http-host/config-files/destination-pattern-map-2.cfg
```

Related Commands

Command	Description
destination e164-pattern-map	Links a destination E.164 pattern map to a dial peer.
url	Specifies the URL of a text file that has E.164 patterns configured on an E.164 pattern map.

show voice class e164-translation

To display the configuration of a voice class E.164 translation table, use the **show voice class e164-translation** command in privileged EXEC mode.

show voice class e164-translation *tag*

Syntax Description

tag	Displays the status and content of the voice class E.164 translation table. The range is from 1 to 10000.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
IOS XE Fuji Release 16.8.1	This command was introduced.

Examples

The following example displays the E.164 translation table. The incoming call numbers +41993000000 and +41993000001 are translated, and replaced by +418893000000 and +418893000001 respectively.

```
Router#show voice class e164-translation
Voice class e164-translation: 1         AdminStat: Up
 Description:
 URL: ftp://test:test123@8.0.0.200/test_e164.cfg
      (Loaded:TRUE Valid: TRUE)

 Duplicate error count:    0
 Syntax error count:    0
 Error count:    0

 Total Translation Rules: 2

 Rule#  Match Call Number                Replace Call Number
 -----  -----------------                -------------------
 1      +41993000000                     +418893000000
 2      +41993000001                     +418893000001

 Total Rules from Internal Sorted list: 2

 Match Reverse Call Number         Match Call Number
 -------------------------         -----------------
 00000039914+                      +41993000000
 10000039914+                      +41993000001


 Lookup Array Setup:

 Offset  Match Reverse Number              Match Call Number
 ------  -------------------              -----------------
 12      00000039914+                     +41993000000
```

Related Commands

Command	Description
show voice class e164-pattern-map	Displays status of a map and all E.164 patterns in the map.

show voice class phone-proxy

To display the details of the sessions and file buffer function being conducted through the all the phone proxies, use the **show voice class phone-proxy** command in privileged EXEC mode.

show voice class phone-proxy [**file-buffer [detail]** | **sessions**]

Syntax Description

file-buffer	(Optional) Shows the summary of phone proxy file buffer function working status.
detail	(Optional) Shows the details of phone proxy file buffer.
sessions	(Optional) Shows the phone proxy instance mapping status between phone and dial peer signal-address and protocol status.

Command Modes

Privileged EXEC mode

Command History

Release	Modification
15.3(3)M	This command was introduced.
IOS XE Fuji Release 16.8.1	This command was modified. The command was enhanced to display phone proxy file buffer details.

Example

The following example shows sample output from the **show voice class phone-proxy** command:

```
Device# show voice class phone-proxy

Phone-Proxy 'mypp':
 Description: mycluster
   Access Secure: secure
   Tftp-client address: 198.51.100.2
   Tftp-server address: 198.51.100.101
   Capf server address: 198.51.100.101
   CUCM service settings: preserve(default)
   Ctl file name: myctl
   Session-timeout: 180 seconds
   Max-concurrent-sessions: 300
   Current sessions: 10
   Configuration status: complete
   Dialpeers associated:
      Name                      State
      --------------------------------
      dialpeer1                    inactive
      dialpeer2                    active
      dialpeer3                    active
Phone-Proxy 'test':
Description: test-cluster
   Access secure: nonsecure (default)
   Tftp-client address: 10.0.0.2
   Tftp-server address: 10.0.0.1
   Local capf server address: 104.0.0.3
   CUCM service settings: disable
   Ctl file name: ctl_test
```

```
   Session-timeout: 180 seconds
   Max-concurrent-sessions: 300
   Current sessions: 20
   Configuration status: not complete
   Dialpeers associated:
      Name                      State
      --------------------------------
      dialpeer 4                     inactive
      dialpeer 5                     inactive
```

The following shows details of the sessions being conducted through the phone proxy:

```
Device# show voice class phone-proxy sessions
Phone-Proxy 'mypp':
               srcaddr:port         dstaddr:port     vrf
             ------------         -------------    ----
-------------Sessions of Dialpeer dialpeer1-------
 |Access:   10.0.100.11:2000    10.0.100.15:69    test1     |
 |Core  :   192.168.0.2:10002   192.169.0.101:69   global    |
  ------------------------------------------------------------------------
 ------------------------------------------------------------------------
 |Access:   10.0.100.35:2004    10.0.100.15:69    test1     |
 |Core  :   192.168.0.2:10008   192.169.0.101:69   global    |
  ------------------------------------------------------------------------

 |Access:   10.0.100.21:4000    10.0.100.15:69    test1     |
 |Core  :                                                   |
  ------------------------------------------------------------------------

Phone-Proxy 'test':
               srcaddr:port         dstaddr:port     vrf
             ------------         -------------    ----
-------------Sessions of Dialpeer dialpeer1----------------
 |Access:   10.2.100.9:2000      10.2.100.15:69    test1     |
 |Core  :   20.21.21.101:10002   20.21.21.2:69     global    |
  ------------------------------------------------------------------------

 |Access:   10.2.100.21:4000    10.2.100.15:69    test1     |
 |Core  :                                                   |
  ------------------------------------------------------------------------
```

show voice class resource-group

To display the resource group configuration information for a specific resource group or all resource groups, use the **show voice class resource-group** command in privileged EXEC mode.

show voice class resource-group {*tag* | **all**}

Syntax Description

tag	Unique tag for the resource group.
all	Displays information for all voice resource groups.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
15.1(2)T	This command was introduced.

Usage Guidelines

You can use the **show voice class resource-group** command to display the parameters configured to monitor resources.

Examples

The following is sample output from the **show voice class resource-group** command:

```
Router> enable
Router# show voice class resource-group 2
Resource Availability Indicator status
Resource Index 2
Resource Type:SYSTEM
         Status: Low threshold
Resource Type: MEM Subtype: io-mem Low/High watermark: 2/5
         Status: Low threshold
Report Interval 34
------------------------------------------------------------
```

The table below describes the significant fields shown in the display.

Table 178: show voice class resource-group Field Descriptions

Field	Description
Resource Index	Unique index value to identify the resource group.
Resource Type	Type of the resource being monitored.
Status	Status of the resource.
Subtype	Subtype of the resource being monitored.
Report Interval	Periodic reporting interval for the resource being monitored. The status of the resource being monitored is reported based on the preconfigured timer value.

Related Commands

Command	Description
debug rai	Enables debugging for Resource Allocation Indication (RAI).
rai target	Configures the SIP RAI mechanism.
resource (voice)	Configures parameters for monitoring resources, use the resource command in voice-class configuration mode.
periodic-report interval	Configures periodic reporting parameters for gateway resource entities.
voice class resource-group	Enters voice-class configuration mode and assigns an identification tag number for a resource group.

show voice class server-group

To display the configurations for all configured server groups or a specified server group, use the **show voice class server-group** command in privileged EXEC mode.

show voice class server-group [*server-group-id* | **dialpeer** *dialpeer-tag* **]**

server-group-id	Unique server group ID to identify the server group.
dialpeer *dialpeer-tag*	Unique number of a dialpeer that is associated with a server group.

Command Modes

User EXEC (>)
Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Release 3.11S 15.4(1)T	The following commands were introduced or modified: **voice class server-group**, **description**, **ipv4 port preference**, **ipv6 port preference**, **hunt-scheme**, **show voice class server-group**, **shutdown (Server Group)**.
Cisco IOS XE Bengaluru 17.4.1a	The following command is introduced under **voice class server-group**. **huntstop** *rule-tag* **resp-code** *from_resp_code* to *to_resp_code*.

Usage Guidelines

You can use the **show voice class server-group** command to display the configurations for all configured server groups or a specified server group.

The following is sample output from the **show voice class server-group** command:

```
Router> enable
Router# show voice class server-group 1
    AdminStatus: Up              OperStatus: Up
            Hunt-Scheme: preference      Last returned server:
            Description: server-group for huntstop feature testing
            Total Huntstop tags: 1
            Tag ID From Response code       To Response code
            ------ -------------------      ------------------
             1     404                      404
             2     410                      599
            -------------------------------------
            Total server entries: 3
            Pref     Type    IP Address      IP Port
            ------------------------------------------------------
            1         ipv4     10.1.1.1
            2         ipv4     10.1.1.2                34515
            3         ipv4     10.1.1.3
```

The table below describes the significant fields shown in the display.

Table 179: show voice class server-group Field Descriptions

Field	Description
description	Description of the server group.

Field	Description
ipv4 port preference	A server IPv4 address as a part of this server group along with an optional port number and preference order.
ipv6 port preference	A server IPv6 address as a part of this server group along with an optional port number and preference order.
hunt-scheme	A hunt method for the order of selection of target server IP addresses (from the IP addresses configured for this server group) for the setting up of outgoing calls.
hunt-stop	Stops hunting based on (configurable) response codes in the Server Group along with dial-peer.

Related Commands

Command	Description
voice class server-group	Enters voice-class configuration mode and configures server groups (groups of IPv4 and IPv6 addresses), description, hunt-scheme, huntstop, and shutdown (Server Group).

show voice class sip-options-keepalive

To display the details of connectivity between CUBE VoIP dial peers and SIP servers, use **show voice class sip-options-keepalive** command in privileged EXEC mode.

show voice class sip-options-keepalive [**global** | *profile-tag*]

global	Displays information on voice class sip-options-keepalive global.
profile-tag	The unique tag for SIP options keepalive profile. Range: 1–10000.

Command Modes

User EXEC (>)

Privileged EXEC (#)

Command History

Release	Modification
IOS XE Fuji Release 16.8.1	This command was introduced.

Usage Guidelines

Use **show voice class sip-options-keepalive global** command to view the global and the instant status information of the out-of-dialog (OOD) ping mechanism that is configured between the dial peers and SIP servers.

Examples

The following sample output displays the details of the server group and the OOD Keepalive Profiles defined on the server group.

```
Router# show voice class sip-options-keepalive global
Server Group: 1
  List of OOD Keepalive Profile(s):
        171
-----------------------------------------------------
```

Related Commands

voice-class sip options-keepalive	Monitors connectivity between CUBE VoIP dial-peers and SIP servers. This command also configures OOD ping mechanism between any number of destinations.

show voice class sip-predefined-profiles

To display the SIP profiles defined on a CUBE router, use **show voice class sip-predefined-profiles** command in privileged EXEC mode.

show voice class sip-predefined-profiles

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
IOS XE Fuji Release 16.8.1	This command was introduced.

Usage Guidelines

The SIP profiles enable SIP messaging between incompatible devices on the network. Use this command to display the SIP profiles defined on all CUBE routers in a network.

Examples

The following sample output displays detailed information about all predefined SIP profiles:

```
Router# show voice class sip-predefined-profiles
voice class sip-hdr-passthrulist 20001
passthru-hdr Call-Info
passthru-hdr Content-ID
passthru-hdr Allow-Events
passthru-hdr Supported
passthru-hdr Remote-Party-I
passthru-hdr Require
passthru-hdr Referred-By

voice class sip-profiles 20001
  request INVITE sip-header Cisco-Guid remove
```

show voice class uri

To display summary or detailed information about configured uniform resource identifier (URI) voice classes, use the **show voice class uri** command in user EXEC or privileged EXEC mode.

show voice class uri [*tag* | **summary**]

Syntax Description

tag	(Optional) Specific URI voice class for which to display detailed information.
summary	(Optional) Displays a short summary of all URI voice classes.

Command Default

Detailed information about the configured URI voice classes is displayed.

Command Modes

User EXEC (>)
Privileged EXEC (#)

Command History

Release	Modification
12.3(4)T	This command was introduced.
15.1(2)T	This command was modified. The command was enhanced to display the mutiple hosts in the configured URI classes.

Usage Guidelines

If both the *tag* argument and **summary** keyword are omitted, the output displays detailed information about all URI voice classes.

Examples

The following is sample output from this command:

```
Router# show voice class uri
Voice URI class: 100
     SNMP status = Active
     Schema = sip
     pattern = 12345
Voice URI class: 101
     SNMP status = Active
     Schema = sip
     pattern = 555....
Voice URI class: 102
     SNMP status = Active
     Schema = sip
     user-id = demo
     host = cisco
     phone context =
Voice URI class: 103
    SNMP status = Active
    Schema = tel
    phone number = 555....
    phone context =
Voice URI class: 700
     SNMP status = Active
     Schema = sip
     pattern = elmo@sip.tgw.com*
```

```
Voice URI class: 104
     SNMP status = Active
     Schema = tel
     pattern = 5550134
Voice URI class: 700
     SNMP status = Active
     Schema = sip
     user-id =
     host = exmp.example.com
     phone context =

     host instances:
      ipv4:192.168.0.1
      ipv6:[2001:0DB8:0:1:FFFF:1234::5]
      dns:ogw.example.com
```

The following is sample output from this command with the **summary** keyword:

```
Router# show voice class uri summary

_____________________________________________________________
Class Name                      Schema     SNMP
-------------------------------------------------------------
100                             sip       Active
101                             sip       Active
102                             sip       Active
103                             tel       Active
700                             sip       Active
104                             tel       Active
_____________________________________________________________
```

The table below describes the significant fields in the displays.

Table 180: show voice class uri Field Descriptions

Field	Description
Class Name	Tag that identifies the URI voice class.
Schema	Whether the voice class is used for SIP or TEL URIs.
pattern	Pattern used to match the entire SIP or TEL URI as configured with the **pattern** command.
user-id	Pattern used to match the user-id field in the SIP URI as configured with the **user-id** command.
host	Pattern used to match the host field in the SIP URI with the **host** command.
phone number	Pattern used to match the phone number field in a TEL URI as configured with the **phone number** command.
phone context	Pattern used to match the phone context field in a SIP or TEL URI as configured with the **phone context** command.

Related Commands

Command	Description
debug voice uri	Displays debugging messages related to URI voice classes.
show dialplan incall uri	Displays which dial peer is matched for a specific URI in an incoming call.

Command	Description
show dialplan uri	Displays which outbound dial peer is matched for a specific destination URI.
voice class uri	Creates or modifies a voice class for matching dial peers to calls containing a SIP or TEL URI.

show voice connectivity summary

To display the results of the last connectivity checks performed on all analog Foreign Exchange Station (FXS) ports on a router, use the **show voice connectivity summary** command in privileged EXEC mode.

show voice connectivity summary

Syntax Description

This command has no arguments or keywords.

Command Default

A summary of the last connectivity checks performed on all analog FXS ports on a router is displayed.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
15.1(3)T	This command was introduced.

Examples

The following example shows how the **show voice connectivity summary** command is used:

```
Router> enable
Router# show voice connectivity summary
.
.
.
! The summary results include information such as the port address, type of connectivity
! check performed, result of connectivity check for each port
```

show voice data

To display the call control application programming interface (CCAPI) and Telephony Service Provider (VTSP) data structures, use the **show voice data** command in user EXEC or privileged EXEC mode.

show voice data {**ccapi** {**ccCallEntry** {*call-id* | **all**} | **ccCallInfo**} | **vtsp** {**ccCallInfo** | **vtsp_cdb** {*call-id* | **all**}} | **vtsp_sdb** {*call-id* | **all**}}

Syntax Description

ccapi	Displays all the CCAPI calls.
ccCallEntry	Displays the call entry.
call-id	Call identifier (ID) in the range 1 to 4294967295.
all	Displays all the call entries.
ccCallInfo	Displays the call information.
vtsp	Displays all the VTSP calls.
vtsp_cdb	Displays all the VTSP call control back calls.
vtsp_sdb	Displays all the VTSP signalling data block calls.

Command Modes

User EXEC (>)
Privileged EXEC (#)

Command History

Release	Modification
12.4(22)T	This command was introduced in a release earlier than Cisco IOS Release 12.4(22)T.

Examples

The following is sample output from the **show voice data** command:

```
Router# show voice data ccapi ccCallEntry all
CallEntry=0x6B8051B0; CallID=7(0x7)::
element:{ 0x6B8051B0; 0x6B8051B4; 0x6B8051B8; } 7; <appReturnStack>; 1735408; 1; 0x6B8051D8;
 7; 8; callInfo:{ 0; 112233; <NULL>; 889988; <NULL>; <NULL>; <NULL>; <NULL>; <NULL>;
 <NULL>; FALSE; FALSE; TRUE; <NULL>; 0; 0; 0; <NULL>; RegularLine; Unknown;
D356CC33-E54B-11D7-8005-00169D6EE1AE; D356CC33-E54B-11D7-8005-00169D6EE1AE; 0; 0; 0; 0; 0;
 998877; 0x6B80547C; 0; TRUE; FALSE; 0.0.0.0; 0.0.0.0; 0x6B8054A0; 0x6B8054A4; 0x6B8054A8;
 0x6B8054AC; 0; FALSE; FALSE; 0x6B8054BC; 0; call_decode:{ redirect_info:{ 0xFF; 0xFF; 0xFF;
 0xFF; 0xFF; 0xFF; 0x00; 0xFF; 255; <NULL>; <NULL>; 0x00; FALSE; FALSE; } 0x00; 0x80; 0x00;
 0x80; 0; 0x00; <NULL>; 0; 0x00; <NULL>; FALSE; FALSE; FALSE; FALSE; -1; <NULL>; TRUE;
<transfer_info>; FALSE; 129; 40; 104; 0xFF; TRUE; } FALSE;
D357685B-E54B-11D7-8016-CB962D72A90A; 0; 0; 0; 0; 0; 0; 0x6B805634; FALSE; <NULL>; FALSE;
FALSE; FALSE; 0; 0; 0; <NULL>; ISDN 7/0:1:D; FALSE; FALSE; FALSE; 0x00; <NULL>; <NULL>;
0x6B80585C; 0; 0x6B805864; } 0x6B805914; 0x6B805918; 0x6B80591C; 0x6B805920; <altAssocList>;
 FALSE; 0x6B80593C; 0x6B805940; 0x6B805944; FALSE; 0; 65535; TRUE; 0; FALSE; 1;
<disconnect_timer>; <inter_digit_timer>; 10000; <initial_timer_timestamp>; 10000; FALSE;
0; 0; -1; <NULL>; 0x6B8059F8; <evCategoryMask>; <evDetailMask>; 4294967295; 0x6B805C48;
FALSE; 0; 0; TRUE; TRUE; TRUE; 0; 0; 0x6B805C6C; FALSE; 0; 4; 0; -1; FALSE;
CallEntry=0x6B805C90; CallID=8(0x8)::
```

```
element:{ 0x6B805C90; 0x6B805C94; 0x6B805C98; } 8; <appReturnStack>; 1735408; 2; 0x6B805CB8;
 8; 7; callInfo:{ 0; 112233; <NULL>; 889988; <NULL>; 112233; 112233; <NULL>; <NULL>; <NULL>;
 <NULL>; FALSE; FALSE; TRUE; <NULL>; 0; 0; 0; <NULL>; RegularLine; Unknown;
D356CC33-E54B-11D7-8005-00169D6EE1AE; D356CC33-E54B-11D7-8005-00169D6EE1AE; 7; 0; 0; 0; 2;
 112233; 0x6B805F5C; 0; FALSE; FALSE; 0.0.0.0; 0.0.0.0; 0x6B805F80; 0x6B805F84; 0x6B805F88;
 0x6B805F8C; 0; FALSE; FALSE; 0x6B805F9C; 0; call_decode:{ redirect_info:{ 0xFF; 0xFF; 0xFF;
 0xFF; 0xFF; 0xFF; 0x00; 0xFF; 255; <NULL>; <NULL>; 0x00; FALSE; FALSE; } 0x00; 0x80; 0x00;
 0x00; 0; 0x00; <NULL>; 0; 0x00; <NULL>; FALSE; FALSE; FALSE; FALSE; -1; <NULL>; TRUE;
<transfer_info>; FALSE; 129; 40; 104; 0xFF; TRUE; } FALSE;
D357685B-E54B-11D7-8016-CB962D72A90A; 0; 0; -1; 0; 0; 0; 0x6B806114; FALSE; <NULL>; FALSE;
 FALSE; FALSE; 0; 0; 0; <NULL>; ISDN 7/0:1:D; TRUE; FALSE; FALSE; 0x00; <NULL>; <NULL>;
0x6B80633C; 0; 0x6B806344; } 0x6B8063F4; 0x6B8063F8; 0x6B8063FC; 0x6B806400; <altAssocList>;
 FALSE; 0x6B80641C; 0x6B806420; 0x6B806424; FALSE; 0; 65535; FALSE; 0; FALSE; 1;
<disconnect_timer>; <inter_digit_timer>; 10000; <initial_timer_timestamp>; 10000; FALSE;
0; 0; -1; <NULL>; 0x6B8064D8; <evCategoryMask>; <evDetailMask>; 4294967295; 0x6B806728;
FALSE; 0; 0; TRUE; TRUE; TRUE; 0; 0; 0x6B80674C; FALSE; 0; 4; 0; -1; FALSE;
```

The table below describes the significant fields shown in the display.

Table 181: show voice data Field Descriptions

Field	Description
CallEntry	Displays the call entry identification number used for the incoming call leg.
CallID	Displays the specified call identifier value.
element	Indicates the various configuration values for the service element.
callInfo	Displays the call informaton.
call_decode	Displays the status of the audio decoder.
redirect_info	Displays the forwarding request information when a call is being forwarded.
transfer_info	Displays the call transfer request information.
disconnect_timer	Displays the timeout value, in seconds, specified to disconnect the call.
inter_digit_timer	Displays the maximum allowable time, in seconds, between digits dialed by the user.

Related Commands

Command	Description
debug voip ccapi error	Traces error logs in the call control API.

show voice dnis-map

To display current dialed-number identification service (DNIS) map information, use the show voice dnis-map command in privileged EXEC mode.

show voice dnis-map [*dnis-map-name* | **summary**]

Syntax Description

dnis -map-name	(Optional) Name of a specific DNIS map.
summary	(Optional) Displays a short summary of each DNIS map.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.2(2)XB	This command was introduced on the Cisco AS5300, Cisco AS5350, and Cisco AS5400.
12.2(11)T	This command was integrated into Cisco IOS Release 12.2(11)T and implemented on the Cisco 3640 and Cisco 3660.

Usage Guidelines

This command displays a detailed description of each configured DNIS map.

If the name of a specific DNIS map is entered, the command displays detailed information about only that DNIS map.

If the **summary** keyword is used, the command displays a one-line summary about each DNIS map.

If an asterisk is displayed next to a DNIS map name when the **summary** keyword is used, it means that the DNIS map is configured, but not running. Normally this is because the external text file was not successfully loaded, for example:

```
dnis-map            Entries    URL
--------            -------    ---
dmap1               1
*dmap4              0          http://dnismaps/dnismap4.txt
```

To create a DNIS map, use the **voice dnis-map** command. You can link to an external DNIS map text file or use the **dnis** command to add numbers to a DNIS map in Cisco IOS software.

To associate a DNIS map with a dial peer, use the **dnis-map** command.

Examples

The following is sample output from the show voice dnis-map command:

```
Router# show voice dnis-map
There are 2 dnis-maps configured
Dnis-map dmap1
----------------------------------------
  It has 3 entries
  It is not populated from a file.
DNIS                URL
----                ---
 4085551212         tftp://global/tickets/movies.vxml
```

```
 4085551234           tftp://global/tickets/plays.vxml
 4085554321           tftp://global/tickets/games.vxml
Dnis-map dmap4
----------------------------------------
  It has 0 entries
  It is populated from url http://dnismaps/dnismap4.txt
DNIS               URL
----               ---
```

The table below describes the fields shown in this output.

Table 182: show voice dnis-map Field Descriptions

Field	Description
Dnis-map	Name of a DNIS map that is configured on the gateway.
DNIS	Destination telephone number specified in this DNIS map.
URL	Location of the VoiceXML document to invoke for this DNIS number.

The following is sample output from the show voice dnis-map **summary**command:

```
Router# show voice dnis-map summary
There are 3 dnis-maps configured
dnis-map           Entries    URL
--------           -------    ---
dmap1              3
dmap4              0        http://dnismaps/dnismap4.txt
dmap6              8
```

describes the fields shown in this output.

Table 183: show voice dnis-map summary Field Descriptions

Field	Description
dnis-map	Names of the DNIS maps that are configured on the gateway.
Entries	Number of entries in DNIS maps that reside on the gateway. This field displays 0 if the DNIS map is a text file stored on an external server.
URL	Location of externally stored DNIS maps.

Related Commands

Command	Description
dnis	Adds a DNIS number to a DNIS map.
dnis -map	Associates a DNIS map to a dial peer.
voice dnis -map	Enters DNIS map configuration mode to create a DNIS map.
voice dnis -map load	Reloads a DNIS map that has changed since the previous load.

show voice dsmp stream

To display the current session of voice Distributed Stream Media Processor (DSPM) media stream, the recent state transitions, and stream connection, use the **show voice dsmp stream** command in privileged EXEC mode.

show voice dsmp stream {*stream ID* | **leg**}

Syntax Description

stream ID	DSMP media stream identifier. Range: 1 to 4294967295.
leg	Call leg corresponding to a caller ID.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.3(14)T	This command was introduced.

Usage Guidelines

When the calls hang, use this command to get the current sessions of the DSMP media stream. You can look at the DSMP state transitions corresponding to the calls and find out the problems.

Examples

The following example shows an output of a typical DSMP session in a VoIP call. This call consists of four streams, two input streams and two output streams:

```
Router# show voice dsmp stream
Total number of streams in use is: 4

Stream information:: stream=1
Type: TDM, Direction: OUTPUT
Fax/Modem Type: voice
Xmit Function: 0x00000000
Xmit function is Enabled
Call ID: 4, Conference ID: -1

Session information:: session=0x658CA948 dsp_intf=0x642DDD8C dsp_name=1/9:3

connections=2 streams=4 (5 1 4 3 )
current state S_DSMP_VC_RUNNING current container simple_voice_container
State Transitions: timestamp (container, state) -- event -> (container, state)
367121.596 (simple_voice_container, S_DSMP_VC_RUNNING) -- E_DSMP_CC_PLAY_REQ ->
(simple_voice_container, CNFSM_NO_STATE_CHANGE)
367121.796 (simple_voice_container, S_DSMP_VC_RUNNING) -- E_DSMP_CC_PLAY_REQ ->
(simple_voice_container, CNFSM_NO_STATE_CHANGE)
367122.712 (simple_voice_container, CNFSM_CONTAINER_STATE) -- E_DSMP_DSP_DTMF_DIGIT_BEGIN
-> (simple_voice_container, CNFSM_NO_STATE_CHANGE)
367122.732 (simple_voice_container, CNFSM_CONTAINER_STATE) -- E_DSMP_DSP_DTMF_DIGIT_END ->
 (simple_voice_container, CNFSM_NO_STATE_CHANGE)
367122.920 (simple_voice_container, CNFSM_CONTAINER_STATE) -- E_DSMP_DSP_DTMF_DIGIT_BEGIN
-> (simple_voice_container, CNFSM_NO_STATE_CHANGE)
367122.940 (simple_voice_container, CNFSM_CONTAINER_STATE) -- E_DSMP_DSP_DTMF_DIGIT_END ->
 (simple_voice_container, CNFSM_NO_STATE_CHANGE)
367123.112 (simple_voice_container, CNFSM_CONTAINER_STATE) -- E_DSMP_DSP_DTMF_DIGIT_BEGIN
```

```
-> (simple_voice_container, CNFSM_NO_STATE_CHANGE)
367123.152 (simple_voice_container, CNFSM_CONTAINER_STATE) -- E_DSMP_DSP_DTMF_DIGIT_END ->
 (simple_voice_container, CNFSM_NO_STATE_CHANGE)
367124.432 (simple_voice_container, S_DSMP_VC_RUNNING) -- E_DSMP_CC_PLAY_REQ ->
(simple_voice_container, CNFSM_NO_STATE_CHANGE)
367124.632 (simple_voice_container, S_DSMP_VC_RUNNING) -- E_DSMP_CC_PLAY_REQ ->
(simple_voice_container, CNFSM_NO_STATE_CHANGE)
367124.732 (simple_voice_container, S_DSMP_VC_RUNNING) -- E_DSMP_CC_PLAY_REQ ->
(simple_voice_container, CNFSM_NO_STATE_CHANGE)
367124.932 (simple_voice_container, S_DSMP_VC_RUNNING) -- E_DSMP_CC_PLAY_REQ ->
(simple_voice_container, CNFSM_NO_STATE_CHANGE)
367125.032 (simple_voice_container, S_DSMP_VC_RUNNING) -- E_DSMP_CC_PLAY_REQ ->
(simple_voice_container, CNFSM_NO_STATE_CHANGE)
367125.232 (simple_voice_container, S_DSMP_VC_RUNNING) -- E_DSMP_CC_PLAY_REQ ->
(simple_voice_container, CNFSM_NO_STATE_CHANGE)
367126.140 (simple_voice_container, CNFSM_CONTAINER_STATE) -- E_DSMP_DSP_DTMF_DIGIT_BEGIN
-> (simple_voice_container, CNFSM_NO_STATE_CHANGE)
367126.160 (simple_voice_container, CNFSM_CONTAINER_STATE) -- E_DSMP_DSP_DTMF_DIGIT_END ->
 (simple_voice_container, CNFSM_NO_STATE_CHANGE)
367126.340 (simple_voice_container, CNFSM_CONTAINER_STATE) -- E_DSMP_DSP_DTMF_DIGIT_BEGIN
-> (simple_voice_container, CNFSM_NO_STATE_CHANGE)
367126.380 (simple_voice_container, CNFSM_CONTAINER_STATE) -- E_DSMP_DSP_DTMF_DIGIT_END ->
 (simple_voice_container, CNFSM_NO_STATE_CHANGE)
367126.548 (simple_voice_container, CNFSM_CONTAINER_STATE) -- E_DSMP_DSP_DTMF_DIGIT_BEGIN
-> (simple_voice_container, CNFSM_NO_STATE_CHANGE)
367126.568 (simple_voice_container, CNFSM_CONTAINER_STATE) -- E_DSMP_DSP_DTMF_DIGIT_END ->
 (simple_voice_container, CNFSM_NO_STATE_CHANGE)

Session log information::
Regular Timer:
    Timer start operations:
             Timestamp    Duration(ms)        Caller
            367122.652            4000    0x6113397C
            367119.388            4000    0x6113397C
            367117.624           10000    0x6112ED88

    Timer stop operations:
             Timestamp    Duration(ms)        Caller
            367122.656               0    0x61133A98
            367119.392               0    0x61133A98
            367117.624               0    0x6112F060
            367117.624               0    0x6112EE24
    Number of overwritten entries: 2

Periodic Timer:
    Timer start operations:
    None
    Timer stop operations:
    None
Packet suppression is disabled

Stream information:: stream=3
Type: PACKET, Direction: OUTPUT
Fax/Modem Type: voice
Xmit Function: 0x6111D324
Xmit function is Enabled
Call ID: 3, Conference ID: 2
DSP Encap: 0x1
Codec Mask: 0x4; Codec Bytes: 20
Fax Rate Mask: 0x2; Fax Bytes: 20; T38 Disabled
VAD Mask: 0x2

Session information:: session=0x658CA948 dsp_intf=0x642DDD8C dsp_name=1/9:3
```

```
connections=2 streams=4 (5 1 4 3 )
current state S_DSMP_VC_RUNNING current container simple_voice_container
State Transitions: timestamp (container, state) -- event -> (container, state)
367128.452 (simple_voice_container, S_DSMP_VC_RUNNING) -- E_DSMP_CC_PLAY_REQ ->
(simple_voice_container, CNFSM_NO_STATE_CHANGE)
367128.652 (simple_voice_container, S_DSMP_VC_RUNNING) -- E_DSMP_CC_PLAY_REQ ->
(simple_voice_container, CNFSM_NO_STATE_CHANGE)
367129.556 (simple_voice_container, CNFSM_CONTAINER_STATE) -- E_DSMP_DSP_DTMF_DIGIT_BEGIN
-> (simple_voice_container, CNFSM_NO_STATE_CHANGE)
367129.588 (simple_voice_container, CNFSM_CONTAINER_STATE) -- E_DSMP_DSP_DTMF_DIGIT_END ->
 (simple_voice_container, CNFSM_NO_STATE_CHANGE)
367129.756 (simple_voice_container, CNFSM_CONTAINER_STATE) -- E_DSMP_DSP_DTMF_DIGIT_BEGIN
-> (simple_voice_container, CNFSM_NO_STATE_CHANGE)
367129.796 (simple_voice_container, CNFSM_CONTAINER_STATE) -- E_DSMP_DSP_DTMF_DIGIT_END ->
 (simple_voice_container, CNFSM_NO_STATE_CHANGE)
367129.968 (simple_voice_container, CNFSM_CONTAINER_STATE) -- E_DSMP_DSP_DTMF_DIGIT_BEGIN
-> (simple_voice_container, CNFSM_NO_STATE_CHANGE)
367129.988 (simple_voice_container, CNFSM_CONTAINER_STATE) -- E_DSMP_DSP_DTMF_DIGIT_END ->
 (simple_voice_container, CNFSM_NO_STATE_CHANGE)
367131.276 (simple_voice_container, S_DSMP_VC_RUNNING) -- E_DSMP_CC_PLAY_REQ ->
(simple_voice_container, CNFSM_NO_STATE_CHANGE)
367131.472 (simple_voice_container, S_DSMP_VC_RUNNING) -- E_DSMP_CC_PLAY_REQ ->
(simple_voice_container, CNFSM_NO_STATE_CHANGE)
367131.572 (simple_voice_container, S_DSMP_VC_RUNNING) -- E_DSMP_CC_PLAY_REQ ->
(simple_voice_container, CNFSM_NO_STATE_CHANGE)
367131.772 (simple_voice_container, S_DSMP_VC_RUNNING) -- E_DSMP_CC_PLAY_REQ ->
(simple_voice_container, CNFSM_NO_STATE_CHANGE)
367131.872 (simple_voice_container, S_DSMP_VC_RUNNING) -- E_DSMP_CC_PLAY_REQ ->
(simple_voice_container, CNFSM_NO_STATE_CHANGE)
367132.072 (simple_voice_container, S_DSMP_VC_RUNNING) -- E_DSMP_CC_PLAY_REQ ->
(simple_voice_container, CNFSM_NO_STATE_CHANGE)
367132.980 (simple_voice_container, CNFSM_CONTAINER_STATE) -- E_DSMP_DSP_DTMF_DIGIT_BEGIN
-> (simple_voice_container, CNFSM_NO_STATE_CHANGE)
367133.000 (simple_voice_container, CNFSM_CONTAINER_STATE) -- E_DSMP_DSP_DTMF_DIGIT_END ->
 (simple_voice_container, CNFSM_NO_STATE_CHANGE)
367133.180 (simple_voice_container, CNFSM_CONTAINER_STATE) -- E_DSMP_DSP_DTMF_DIGIT_BEGIN
-> (simple_voice_container, CNFSM_NO_STATE_CHANGE)
367133.220 (simple_voice_container, CNFSM_CONTAINER_STATE) -- E_DSMP_DSP_DTMF_DIGIT_END ->
 (simple_voice_container, CNFSM_NO_STATE_CHANGE)
367133.400 (simple_voice_container, CNFSM_CONTAINER_STATE) -- E_DSMP_DSP_DTMF_DIGIT_BEGIN
-> (simple_voice_container, CNFSM_NO_STATE_CHANGE)
367133.420 (simple_voice_container, CNFSM_CONTAINER_STATE) -- E_DSMP_DSP_DTMF_DIGIT_END ->
 (simple_voice_container, CNFSM_NO_STATE_CHANGE)

Session log information::
Regular Timer:
    Timer start operations:
             Timestamp    Duration(ms)        Caller
            367131.020            4000    0x6113397C
            367128.316            4000    0x6113397C
            367122.652            4000    0x6113397C
            367119.388            4000    0x6113397C
    Number of overwritten entries: 1

    Timer stop operations:
             Timestamp    Duration(ms)        Caller
            367131.024               0    0x61133A98
            367128.320               0    0x61133A98
            367122.656               0    0x61133A98
            367119.392               0    0x61133A98
    Number of overwritten entries: 4

Periodic Timer:
    Timer start operations:
```

```
    None
    Timer stop operations:
    None
Packet suppression is disabled

Stream information:: stream=4
Type: PACKET, Direction: INPUT
Fax/Modem Type: voice
Xmit Function: 0x61F2CA34
Xmit function is Enabled
Call ID: 3, Conference ID: 2
DSP Encap: 0x1
Codec Mask: 0x4; Codec Bytes: 20
Fax Rate Mask: 0x2; Fax Bytes: 20; T38 Disabled
VAD Mask: 0x2

Session information:: session=0x658CA948 dsp_intf=0x642DDD8C dsp_name=1/9:3

connections=2 streams=4 (5 1 4 3 )
current state S_DSMP_VC_RUNNING current container simple_voice_container
State Transitions: timestamp (container, state) -- event -> (container, state)
367133.400 (simple_voice_container, CNFSM_CONTAINER_STATE) -- E_DSMP_DSP_DTMF_DIGIT_BEGIN
-> (simple_voice_container, CNFSM_NO_STATE_CHANGE)
367133.420 (simple_voice_container, CNFSM_CONTAINER_STATE) -- E_DSMP_DSP_DTMF_DIGIT_END ->
 (simple_voice_container, CNFSM_NO_STATE_CHANGE)
367134.692 (simple_voice_container, S_DSMP_VC_RUNNING) -- E_DSMP_CC_PLAY_REQ ->
(simple_voice_container, CNFSM_NO_STATE_CHANGE)
367134.892 (simple_voice_container, S_DSMP_VC_RUNNING) -- E_DSMP_CC_PLAY_REQ ->
(simple_voice_container, CNFSM_NO_STATE_CHANGE)
367134.992 (simple_voice_container, S_DSMP_VC_RUNNING) -- E_DSMP_CC_PLAY_REQ ->
(simple_voice_container, CNFSM_NO_STATE_CHANGE)
367135.192 (simple_voice_container, S_DSMP_VC_RUNNING) -- E_DSMP_CC_PLAY_REQ ->
(simple_voice_container, CNFSM_NO_STATE_CHANGE)
367135.292 (simple_voice_container, S_DSMP_VC_RUNNING) -- E_DSMP_CC_PLAY_REQ ->
(simple_voice_container, CNFSM_NO_STATE_CHANGE)
367135.492 (simple_voice_container, S_DSMP_VC_RUNNING) -- E_DSMP_CC_PLAY_REQ ->
(simple_voice_container, CNFSM_NO_STATE_CHANGE)
367136.400 (simple_voice_container, CNFSM_CONTAINER_STATE) -- E_DSMP_DSP_DTMF_DIGIT_BEGIN
-> (simple_voice_container, CNFSM_NO_STATE_CHANGE)
367136.432 (simple_voice_container, CNFSM_CONTAINER_STATE) -- E_DSMP_DSP_DTMF_DIGIT_END ->
 (simple_voice_container, CNFSM_NO_STATE_CHANGE)
367136.600 (simple_voice_container, CNFSM_CONTAINER_STATE) -- E_DSMP_DSP_DTMF_DIGIT_BEGIN
-> (simple_voice_container, CNFSM_NO_STATE_CHANGE)
367136.640 (simple_voice_container, CNFSM_CONTAINER_STATE) -- E_DSMP_DSP_DTMF_DIGIT_END ->
 (simple_voice_container, CNFSM_NO_STATE_CHANGE)
367136.812 (simple_voice_container, CNFSM_CONTAINER_STATE) -- E_DSMP_DSP_DTMF_DIGIT_BEGIN
-> (simple_voice_container, CNFSM_NO_STATE_CHANGE)
367136.840 (simple_voice_container, CNFSM_CONTAINER_STATE) -- E_DSMP_DSP_DTMF_DIGIT_END ->
 (simple_voice_container, CNFSM_NO_STATE_CHANGE)
367138.112 (simple_voice_container, S_DSMP_VC_RUNNING) -- E_DSMP_CC_PLAY_REQ ->
(simple_voice_container, CNFSM_NO_STATE_CHANGE)
367138.312 (simple_voice_container, S_DSMP_VC_RUNNING) -- E_DSMP_CC_PLAY_REQ ->
(simple_voice_container, CNFSM_NO_STATE_CHANGE)
367138.412 (simple_voice_container, S_DSMP_VC_RUNNING) -- E_DSMP_CC_PLAY_REQ ->
(simple_voice_container, CNFSM_NO_STATE_CHANGE)
367138.612 (simple_voice_container, S_DSMP_VC_RUNNING) -- E_DSMP_CC_PLAY_REQ ->
(simple_voice_container, CNFSM_NO_STATE_CHANGE)
367138.712 (simple_voice_container, S_DSMP_VC_RUNNING) -- E_DSMP_CC_PLAY_REQ ->
(simple_voice_container, CNFSM_NO_STATE_CHANGE)
367138.912 (simple_voice_container, S_DSMP_VC_RUNNING) -- E_DSMP_CC_PLAY_REQ ->
(simple_voice_container, CNFSM_NO_STATE_CHANGE)

Session log information::
Regular Timer:
```

```
    Timer start operations:
             Timestamp    Duration(ms)        Caller
            367137.648            4000    0x6113397C
            367134.440            4000    0x6113397C
            367131.020            4000    0x6113397C
            367128.316            4000    0x6113397C
    Number of overwritten entries: 3

    Timer stop operations:
             Timestamp    Duration(ms)        Caller
            367137.648               0    0x61133A98
            367134.440               0    0x61133A98
            367131.024               0    0x61133A98
            367128.320               0    0x61133A98
    Number of overwritten entries: 6

Periodic Timer:
    Timer start operations:
    None
    Timer stop operations:
    None
Packet suppression is disabled

Stream information:: stream=5
Type: TDM, Direction: INPUT
Fax/Modem Type: voice
Xmit Function: 0x00000000
Xmit function is Enabled
Call ID: 4, Conference ID: -1

Session information:: session=0x658CA948 dsp_intf=0x642DDD8C dsp_name=1/9:3

connections=2 streams=4 (5 1 4 3 )
current state S_DSMP_VC_RUNNING current container simple_voice_container
State Transitions: timestamp (container, state) -- event -> (container, state)
367138.712 (simple_voice_container, S_DSMP_VC_RUNNING) -- E_DSMP_CC_PLAY_REQ ->
(simple_voice_container, CNFSM_NO_STATE_CHANGE)
367138.912 (simple_voice_container, S_DSMP_VC_RUNNING) -- E_DSMP_CC_PLAY_REQ ->
(simple_voice_container, CNFSM_NO_STATE_CHANGE)
367139.824 (simple_voice_container, CNFSM_CONTAINER_STATE) -- E_DSMP_DSP_DTMF_DIGIT_BEGIN
-> (simple_voice_container, CNFSM_NO_STATE_CHANGE)
367139.844 (simple_voice_container, CNFSM_CONTAINER_STATE) -- E_DSMP_DSP_DTMF_DIGIT_END ->
 (simple_voice_container, CNFSM_NO_STATE_CHANGE)
367140.024 (simple_voice_container, CNFSM_CONTAINER_STATE) -- E_DSMP_DSP_DTMF_DIGIT_BEGIN
-> (simple_voice_container, CNFSM_NO_STATE_CHANGE)
367140.064 (simple_voice_container, CNFSM_CONTAINER_STATE) -- E_DSMP_DSP_DTMF_DIGIT_END ->
 (simple_voice_container, CNFSM_NO_STATE_CHANGE)
367140.244 (simple_voice_container, CNFSM_CONTAINER_STATE) -- E_DSMP_DSP_DTMF_DIGIT_BEGIN
-> (simple_voice_container, CNFSM_NO_STATE_CHANGE)
367140.252 (simple_voice_container, CNFSM_CONTAINER_STATE) -- E_DSMP_DSP_DTMF_DIGIT_END ->
 (simple_voice_container, CNFSM_NO_STATE_CHANGE)
367141.536 (simple_voice_container, S_DSMP_VC_RUNNING) -- E_DSMP_CC_PLAY_REQ ->
(simple_voice_container, CNFSM_NO_STATE_CHANGE)
367141.736 (simple_voice_container, S_DSMP_VC_RUNNING) -- E_DSMP_CC_PLAY_REQ ->
(simple_voice_container, CNFSM_NO_STATE_CHANGE)
367141.836 (simple_voice_container, S_DSMP_VC_RUNNING) -- E_DSMP_CC_PLAY_REQ ->
(simple_voice_container, CNFSM_NO_STATE_CHANGE)
367142.036 (simple_voice_container, S_DSMP_VC_RUNNING) -- E_DSMP_CC_PLAY_REQ ->
(simple_voice_container, CNFSM_NO_STATE_CHANGE)
367142.136 (simple_voice_container, S_DSMP_VC_RUNNING) -- E_DSMP_CC_PLAY_REQ ->
(simple_voice_container, CNFSM_NO_STATE_CHANGE)
367142.336 (simple_voice_container, S_DSMP_VC_RUNNING) -- E_DSMP_CC_PLAY_REQ ->
(simple_voice_container, CNFSM_NO_STATE_CHANGE)
367143.244 (simple_voice_container, CNFSM_CONTAINER_STATE) -- E_DSMP_DSP_DTMF_DIGIT_BEGIN
```

```
-> (simple_voice_container, CNFSM_NO_STATE_CHANGE)
367143.264 (simple_voice_container, CNFSM_CONTAINER_STATE) -- E_DSMP_DSP_DTMF_DIGIT_END ->
 (simple_voice_container, CNFSM_NO_STATE_CHANGE)
367143.444 (simple_voice_container, CNFSM_CONTAINER_STATE) -- E_DSMP_DSP_DTMF_DIGIT_BEGIN
-> (simple_voice_container, CNFSM_NO_STATE_CHANGE)
367143.484 (simple_voice_container, CNFSM_CONTAINER_STATE) -- E_DSMP_DSP_DTMF_DIGIT_END ->
 (simple_voice_container, CNFSM_NO_STATE_CHANGE)
367143.652 (simple_voice_container, CNFSM_CONTAINER_STATE) -- E_DSMP_DSP_DTMF_DIGIT_BEGIN
-> (simple_voice_container, CNFSM_NO_STATE_CHANGE)
367143.672 (simple_voice_container, CNFSM_CONTAINER_STATE) -- E_DSMP_DSP_DTMF_DIGIT_END ->
 (simple_voice_container, CNFSM_NO_STATE_CHANGE)

Session log information::
Regular Timer:
    Timer start operations:
             Timestamp    Duration(ms)        Caller
            367137.648            4000    0x6113397C
            367134.440            4000    0x6113397C
            367131.020            4000    0x6113397C
            367128.316            4000    0x6113397C
    Number of overwritten entries: 3

    Timer stop operations:
             Timestamp    Duration(ms)        Caller
            367137.648               0    0x61133A98
            367134.440               0    0x61133A98
            367131.024               0    0x61133A98
            367128.320               0    0x61133A98
    Number of overwritten entries: 6

Periodic Timer:
    Timer start operations:
    None
    Timer stop operations:
    None
Packet suppression is disabled
```

The table below describes the significant fields shown in the display.

Table 184: show voice dsmp stream Field Descriptions

Field	Description
Stream information	Shows stream ID.
Type	Type of stream.
Direction	Direction of stream.
Fax/Modem Type	Type of fax or modem.
Xmit Function	Transmit function in use.
Call ID	Caller ID of call leg.
Conference ID	Conference ID.
Session information	Information about the associated session.
connections	Number of stream connections.

Field	Description
streams	Number of streams.
current state	Current state and container of the session.
State Transitions	State transitions of the associated session.
DSP Encap	Encapsulation associated with the session.
Codec Mask	Codec mask associated with the session.
Fax Rate Mask	Fax rates associated with the session.
Fax Bytes	Fax bytes associated with the session.
VAD Mask	VAD mask associated with the session.

Related Commands

Command	Description
show call active voice	Displays call information for voice calls in progress.
show voice call	Displays the call status for voice ports on the Cisco router.

show voice dsp

To display either the current status or the selective statistics pertaining to the digital signal processor (DSP) voice channels, use the **show voice dsp** command in User EXEC mode or Privileged EXEC mode.

show voice dsp [**active** [**slot** *slot-number* [*slot-number*]] | **capabilities slot** *slot-number* **dsp** *dsp-number* | **cpu-load slot** *slot-number* **dsp** *dsp-number* [**reset**] | **detailed** | **error** | [**group all** | **sorted-list**] **slot** *slot-number* | **signalling** | **voice** | **version** [*slot* | *slot* **/ dsp**] [*slot* | *slot* **/ dsp**]]

Cisco ASR 1000 Series Routers
show voice dsp [**active** [**slot** *slot-number*] | **capabilities slot** *slot-number* **dsp** *dsp-number* | **cpu-load slot** *slot-number* **dsp** *dsp-number* [**reset**] | **crash-dump** | **detailed** | **error** | **group** { **all** | **slot** *slot-number* } | **signalling** | **sorted-list slot** *slot-number* | **voice**]

Syntax Description

active	(Optional) Displays the active channels.
slot *slot-number* [*slot-number*]	(Optional) Specifies either a single slot or the first slot in a range. To specify a range of slots, enter a **second slot in the syntax of this argument. The second slot specifies the end of the range.** All the slots in the range are affected by the command.
capabilities	(Optional) Displays DSP capabilities.
dsp *dsp-number*	(Optional) Specifies the DSP on the slot.
cpu-load	(Optional) Displays DSP CPU load.
reset	(Optional) Resets DSP CPU statistics.
crash-dump	(Optional) Displays the DSP crash dump status. **Note** To enable a DSP crash dump, set the file limit to a non-zero number, and set the destination to a valid file name.
detailed	(Optional) Displays detailed information about DSP status.
error	(Optional) Displays DSP errors.
group	(Optional) Displays DSP group information.
all	(Optional) Displays all the DSP group details.
sorted-list	(Optional) Displays a DSP-sorted list.
signaling	(Optional) Displays DSP signaling channel usage.
voice	(Optional) Displays DSP voice channel usage.
version	(Optional) Displays the DSP firmware version.

slot	(Optional) The first slot in a range. To specify a range of slots, you can enter a second slot in the syntax of this argument. The second slot specifies the end of the range. All the slots in the range are affected by the command.
/ *dsp*	(Optional) The first DSP in a range. To specify a range of DSPs, you can enter a second DSP in the syntax of this argument. The second DSP specifies the end of the range. All the DSPs in the range are affected by the command. The slash mark is required.

Command Default

No default behavior or values.

Command Modes

User EXEC (>)

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE 17.18.2	This command was implemented on the C8375-E-G2 secure router.
Cisco IOS XE Release 3.3.0S	The **show voice dsp group all** command output was modified for SPA-DSP on the Cisco ASR 1000 Series Router.
Cisco IOS XE Release 3.2S	This command was implemented on the Cisco ASR 1000 Series Router.
Cisco IOS XE Release 2.5	This command was integrated into Cisco IOS XE Release 2.5.
12.4(11)T	The command was modified. Command output was enhanced to display information about the DSP H.320 channels.
12.4(4)XC	The command was modified. The **version** keyword was added and the command was implemented on the Cisco AS5350XM and Cisco AS5400XM platforms.
12.4(4)T	The command was modified. The command output was enhanced to display the codec setting for modem relay operation.
12.3(14)T	The command was modified. The command output was enhanced to display status information pertaining to the NM-HDV network module TI-549 DSPs.
12.1(2)T	This command was integrated into Cisco IOS Release 12.1(2)T.
12.0(7)XK	This command was implemented on the Cisco 2600 Series and Cisco 3600 Series, and the display format was modified.
11.3(1)MA	This command was introduced on the Cisco MC3810.

Usage Guidelines

Use this command when abnormal behavior occurs in the DSP voice channels. The channel or channels should have an active voice call at the time the command is executed.

Cisco ASR 1000 Series Routers

In Cisco IOS XE Release 3.3.0s, the **show voice dsp group all** command output that is displayed when a SPA-DSP undergoes call recovery is enhanced. The command output is seen only during the call recovery process, which lasts for a few milliseconds. The additional information that is included in the command output

pertains to: HA State : DSP_HA_STATE_PENDING1. The additional information is displayed when a SPA-DSP undergoes call recovery.

Examples

The following sample output shows how HA State : DSP_HA_STATE_PENDING1 is added. The additional command output is seen only in Cisco IOS XE Release 3.3.0S and later releases:

```
Router# show voice dsp group all
Show DSP group all

DSP groups on slot 0 bay 0:
dsp 1:
  State: UP
  HA State : DSP_HA_STATE_PENDING1
  Max signal/voice channel: 43/43
  Max credits: 645
  num_of_sig_chnls_allocated: 43
  Transcoding channels allocated: 43
  Group: FLEX_GROUP_XCODE, complexity: LOW
    Shared credits: 0, reserved credits: 645
    Transcoding channels allocated: 24
    Credits used (rounded-up): 360
```

The following sample output shows the current status of the codec, set for modem relay, on channel 1:

```
Router# show voice dsp
----------------------------FLEX VOICE CARD 1 -----------------------------
                           *DSP VOICE CHANNELS*
DSP   DSP              DSPWARE CURR  BOOT                          PAK   TX/RX
TYPE  NUM CH CODEC     VERSION STATE STATE   RST AI VOICEPORT TS ABRT PACK COUNT
===== === == ======== ======= ===== ======= === == ========= == ==== ============
C5510 001 01 modem-re 4.5.909 busy  idle      0  0 1/1/0     05    0      298/353
                           *DSP SIGNALING CHANNELS*
DSP   DSP              DSPWARE CURR  BOOT                          PAK   TX/RX
TYPE  NUM CH CODEC     VERSION STATE STATE   RST AI VOICEPORT TS ABRT PACK COUNT
===== === == ======== ======= ===== ======= === == ========= == ==== ============
C5510 001 05 {flex}   4.5.909 alloc idle      0  0 1/1/3     02    0         15/0
C5510 001 06 {flex}   4.5.909 alloc idle      0  0 1/1/2     02    0         17/0
C5510 001 07 {flex}   4.5.909 alloc idle      0  0 1/1/1     06    0         31/0
C5510 001 08 {flex}   4.5.909 alloc idle      0  0 1/1/0     06    0        321/0
------------------------END OF FLEX VOICE CARD 1 ----------------------------
```

Examples

The following sample output shows the current status of all the DSP voice channels:

```
Router# show voice dsp
DSP# 0, channel# 0 G729A BUSY
DSP# 0, channel# 1 G729A BUSY
DSP# 1, channel# 2 FAX IDLE
DSP# 1, channel# 3 FAX IDLE
DSP# 2, channel# 4 NONE BAD
DSP# 2, channel# 5 NONE BAD
DSP# 3, channel# 6 NONE BAD
DSP# 3, channel# 7 NONE BAD
DSP# 4, channel# 8 NONE BAD
DSP# 4, channel# 9 NONE BAD
DSP# 5, channel# 10 NONE BAD
DSP# 5, channel# 11 NONE BAD
```

Examples

The following is a sample output of this command on a Cisco 1750 router:

```
Router# show voice dsp
DSP#0: state IN SERVICE, 2 channels allocated
channel#0: voice port 1/0, codec G711 ulaw, state UP
channel#1: voice port 1/1, codec G711 ulaw, state UP
DSP#1: state IN SERVICE, 2 channels allocated
channel#0: voice port 2/0, codec G711 ulaw, state UP
channel#1: voice port 2/1, codec G711 ulaw, state UP
DSP#2: state RESET, 0 channels allocated
```

Examples

The following is a sample output command on a secure Survivable Remote Site Telephony (SRST) router with the NM-HDV network module and the TI-549 (C549) DSP installed:

```
Router# show voice dsp
DSP  DSP    DSPWARE  CURR     BOOT                                PAK   TX/RX
TYPE NUM CH CODEC    VERSION  STATE STATE  RST AI VOICEPORT TS ABORT PACK COUNT
==== === == ======== ======= ===== ======= === == ======== === ===== ===========
C549  1  01 {medium} 4.4.3    IDLE  idle     0  0   1/0:0   1   0    9357/9775
C549  1  02 {medium} 4.4.3    IDLE  idle     0      1/0:0   2   0    0/0
C549  2  01 {medium} 4.4.3    IDLE  idle     0  0   1/0:0   3   0    0/0
C549  2  02 {medium} 4.4.3    IDLE  idle     0      1/0:0   4   0    0/0
C549  3  01 {medium} 4.4.3    IDLE  idle     0  0   1/0:0   5   0    0/13
C549  3  02 {medium} 4.4.3    IDLE  idle     0      1/0:0   6   0    0/13
```

Examples

The following is a sample output of this command on an H.320 network configured for video support:

```
Router# show voice dsp

DSP  DSP             DSPWARE CURR  BOOT                           PAK     TX/RX
TYPE NUM CH CODEC    VERSION STATE STATE   RST AI VOICEPORT TS ABORT  PACK COUNT
==== === == ======== ======= ===== ======= === == ========= == ===== ============ edsp 001
 01 g711ulaw  0.1 IDLE  50/0/1.1 edsp 002 02 g711ulaw  0.1 IDLE  50/0/1.2 edsp 003 01 g729r8
 p  0.1 IDLE  50/0/2.1 ----------------------------FLEX VOICE CARD 1
------------------------------
                         *DSP VOICE CHANNELS*
DSP   DSP             DSPWARE CURR  BOOT                            PAK   TX/RX
TYPE  NUM CH CODEC    VERSION STATE STATE   RST AI VOICEPORT TS ABRT PACK COUNT
===== === == ======== ======= ===== ======= === == ========= == ==== ============
C5510 001 05 None     9.0.105 idle  idle      0  0                 0          0/0
C5510 001 06 None     9.0.105 idle  idle      0  0                 0          0/0
C5510 001 07 None     9.0.105 idle  idle      0  0                 0          0/0
C5510 001 08 None     9.0.105 idle  idle      0  0                 0          0/0
C5510 001 09 None     9.0.105 idle  idle      0  0                 0          0/0
C5510 001 10 None     9.0.105 idle  idle      0  0                 0          0/0
C5510 001 11 None     9.0.105 idle  idle      0  0                 0          0/0
C5510 001 12 None     9.0.105 idle  idle      0  0                 0          0/0
C5510 001 13 None     9.0.105 idle  idle      0  0                 0          0/0
C5510 001 14 None     9.0.105 idle  idle      0  0                 0          0/0
C5510 001 15 None     9.0.105 idle  idle      0  0                 0          0/0
C5510 001 16 None     9.0.105 idle  idle      0  0                 0          0/0
C5510 003 01 None     9.0.105 idle  idle      0  0                 0          0/0
C5510 003 02 None     9.0.105 idle  idle      0  0                 0          0/0
C5510 003 03 None     9.0.105 idle  idle      0  0                 0          0/0
C5510 003 04 None     9.0.105 idle  idle      0  0                 0          0/0
C5510 003 05 None     9.0.105 idle  idle      0  0                 0          0/0
C5510 003 06 None     9.0.105 idle  idle      0  0                 0          0/0
```

```
C5510 003 07 None     9.0.105 idle  idle      0  0                 0          0/0
C5510 003 08 None     9.0.105 idle  idle      0  0                 0          0/0
C5510 003 09 None     9.0.105 idle  idle      0  0                 0          0/0
C5510 003 10 None     9.0.105 idle  idle      0  0                 0          0/0
C5510 003 11 None     9.0.105 idle  idle      0  0                 0          0/0
C5510 003 12 None     9.0.105 idle  idle      0  0                 0          0/0
C5510 003 13 None     9.0.105 idle  idle      0  0                 0          0/0
C5510 003 14 None     9.0.105 idle  idle      0  0                 0          0/0
C5510 003 15 None     9.0.105 idle  idle      0  0                 0          0/0
C5510 003 16 None     9.0.105 idle  idle      0  0                 0          0/0
*DSP H.320 CHANNELS*
DSP   DSP     TX/RX       DSPWARE CURR                PAK   TX/RX
TYPE  NUM CH  CODEC       VERSION STATE VOICEPORT TS ABRT PACK COUNT
===== === === =========== ======= ===== ========= == ==== ============
C5510 001 01  h320p(01)   9.0.105 busy  1/0/0:15  06
      001 02  h320s(02)   9.0.105 busy  1/0/0:15  07
      001 03  h320s(03)   9.0.105 busy  1/0/0:15  08
      001 04  h320s(04)   9.0.105 busy  1/0/0:15  09
      001 01a g711ulaw    9.0.105 busy                 0 1013663/5083
                                                                   00
      001 01v h263 /h263  9.0.105 busy                 0 104908/30911
                                                                    4
-----------------------END OF FLEX VOICE CARD 1 ----------------------------
```

The table below describes the significant fields shown in the displays.

Table 185: show voice dsp Field Descriptions

Field	Description
DSP	Number of the DSP.
channel	Number of the channel and its status.
DSP TYPE	TI-549 (C549) DSP.
DSP NUM	Number of the DSP.
CH	Channel number.
CODEC	Complexity setting.
DSPWARE VERSION	Version of DSPware.
CURR STATE	Current status of the channel: alloc (allocated), busy, or idle.
BOOT STATE	DSP readiness, either idle or in service.
RST	Number of times the DSP has been reset or restarted.
AI	Alarm indication count on the channel.
VOICEPORT	Voice card number and slot.
TS	Time slot.
PAK ABORT	Number of dropped packets.
TX/RX PACK COUNT	Number of transmitted and received packets.

C8375-E-G2 router platform

The following output shows the active DSP group information of the C8375-E-G2 router platform:

```
Router# show voice dsp group
         DSP groups on vdsp
         DSP default version: 0.1.717

         dsp 1:
             State: UP, firmware version: 1.0.827
             Max voice channel: 400
             Max credits: 6000, Voice credits: 6000  Transcoding channels allocated: 10
**
             Group: FLEX_GROUP_VOICE, complexity: FLEX
         dsp 2:
             State: UP, firmware version: 1.0.827
             Max voice channel: 400
```

The following example shows the channel capabilities of the DSP profiles on C8375-E-G2 router platform:

```
router# show voice dsp capabilities

Supported vDSP profiles are:
vDSP-32 (Max credits 3360)
vDSP-64 (Max credits 6720)
vDSP-256 (Max credits 26880)
vDSP-512 (Max credits 53760)
vDSP-1024 (Max credits 107520)
vDSP-2048 (Max credits 215040)

Current active vDSP profile is vDSP-500

Credit Information:

Transcode Credit:
LC (G711) Credits: 105
MC (G722/G729a) Credits: 240
HC (iLBC/G729) Credits: 420
VHC (iSAC/Opus) Credits: 420

Universal Transcode Credit:
LC (G711) Credits: 105
MC (G722/G729a) Credits: 336
HC (iLBC/G729) Credits: 672
VHC (iSAC/Opus) Credits: 840

Conference 8-party credits:
LC (G711) Credits: 420
MC (G722) Credits: 672
HC (G729/G729a) Credits: 1120
VHC (iLBC) Credits: 1120

Add-on advanced service:
NR/Ext-NR : 82
ASP : 82

Total of 2 DSPs, each with 26250 credits.
```

Cisco ASR 1000 Series Router

The following sample output shows the DSP Type, DSP number, channel number, codecs running, DSP firmware version, and current state of the channels running on the SPA-DSP inside the Cisco ASR 1000 Series Router:

```
Router# show voice dsp

------------------------------ SPA-DSP 1/1 ---------------------------
*DSP INFORMATION*
DSP    DSP                DSPWARE CURR
TYPE   NUM CH CODEC       VERSION STATE RST AI
====== === == ========= ======== ===== === ==
SP2600 001    None       26.07.00 up    4   0
SP2600 002    None       26.07.00 up    3   0
SP2600 003    None       26.07.00 up    3   0
SP2600 004    None       26.07.00 up    1   0
SP2600 005    None       26.07.00 up    1   0
SP2600 006    None       26.07.00 up    1   0
SP2600 007    None       26.07.00 up    1   0
SP2600 008    None       26.07.00 up    1   0
SP2600 009    None       26.07.00 up    1   0
SP2600 010    None       26.07.00 up    1   0
SP2600 011    None       26.07.00 up    1   0
SP2600 012    None       26.07.00 up    1   0
SP2600 013    None       26.07.00 up    1   0
SP2600 014    None       26.07.00 up    1   0
SP2600 015    None       26.07.00 up    1   0
SP2600 016    None       26.07.00 up    1   0
SP2600 017    None       26.07.00 up    1   0
SP2600 018    None       26.07.00 up    1   0
SP2600 019    None       26.07.00 up    1   0
SP2600 020    None       26.07.00 up    1   0
SP2600 021    None       26.07.00 up    1   0
------------------------- END OF SPA-DSP 1/1 -------------------------------------
```

The following output shows the active channels on SPA-DSP located in slot 1 of the Cisco ASR 1000 Series Router:

```
Router# show voice dsp active slot 1
------------------ SPA-DSP 1/1 ---------------------------
*DSP VOICE CHANNELS*
DSP    DSP                DSPWARE CURR
TYPE   NUM CH CODEC       VERSION STATE RST AI
====== === == ========= ======== ===== === ==
SP2600 001 01 g711ulaw   26.07.00 busy  4   0
SP2600 002 01 g711ulaw   26.07.00 busy  3   0
------------------------- END OF SPA-DSP 1/1 ------------
```

The following example shows the channel capabilities of the different types of codecs on the Cisco ASR 1000 Series Router:

```
Router# show voice dsp capabilities slot 1
Card 1/1 DSP 1 Capabilities:
DSP Type: SP2600 - 43
    Credits   645 ,  G711Credits 15,  HC Credits  37,  MC Credits  23,
    FC Channel  43,  HC Channel  17,  MC Channel  28,
```

```
    Conference 8-party credits:
     G711  58 ,  G729  107,  G722  129,  ILBC  215
  Secure Credits:
    Sec LC Xcode  24,      Sec HC Xcode  64,
    Sec MC Xcode  35,      Sec G729 conf 161,
    Sec G722 conf 215,     Sec ILBC conf 322,
    Sec G711 conf 92 ,
  Max Conference Parties per DSP:
    G711 88,  G729 48,  G722 40,  ILBC 24,
    Sec G711 56,  Sec G729 32,
    Sec G722 24  Sec ILBC 16,
  Voice Channels:
    g711perdsp = 43,  g726perdsp = 28, g729perdsp = 17, g729aperdsp = 28,
    g723perdsp = 17,  g728perdsp = 17, g723perdsp = 17, gsmperdsp   = 28,
    gsmefrperdsp = 17, gsmamrnbperdsp = 17,
    ilbcperdsp = 17, isacperdsp = 8  modemrelayperdsp = 17,
    g72264Perdsp = 28, h324perdsp = 17,
    m_f_thruperdsp = 43, faxrelayperdsp = 28,
    maxchperdsp = 43, minchperdsp = 17,
    srtp_maxchperdsp = 27, srtp_minchperdsp = 14, faxrelay_srtp_perdsp =
4,
    g711_srtp_perdsp = 27, g729_srtp_perdsp = 14, g729a_srtp_perdsp = 24,----------
```

The following example shows the details of the DSP errors on the Cisco ASR 1000 Series Router.

Note The crash dump details must be enabled to display the crash dump for a SPA-DSP. To enable a crash dump, set the destination of the crash dump file to a valid file name, and set the file limit to a non-zero number.

```
Router# show voice dsp crash-dump
Voice DSP Crash-dump status:
    Destination file url is <none>
    File limit is 0
DSP crash dump is currently disabled
To enable DSP crash dump, set file-limit to a non-zero number and set
destination to a valid file name
```

Related Commands

Command	Description
dsp services dspfarm	Enables the DSP farm services.
dspfarm profile	Enters the DSP farm profile configuration mode and defines a profile for DSP farm services.
show dspfarm	Displays DSP farm service information, such as operational status, and DSP resource allocation for transcoding.

show voice dsp channel

To display the voice digital signal processor (DSP) channels, use the **show voice dsp channel**command in user EXEC or privileged EXEC mode.

show voice dsp channel {**operational-status** {*slot* | */dsp* | */channel*} [*slot* | */dsp* | */channel*] | **statistics** *slot-number* [*slot-number*] | **traffic** *slot-number* [*slot-number*]}

Syntax Description

operational-status	Displays the operational state for active sessions on a specific channel or range of channels.
slot	A single slot or the first slot in a range. To specify a range of slots, you can enter a **second slot in the syntax of this argument. The second slot specifies the end of the range.** All slots in the range are affected by the command.
/ *dsp*	A single DSP on the slot or the first DSP in a range. To specify a range of DSPs, you can enter a **second DSP in the syntax of this argument. The second DSP specifies the end of the range.** All DSPs in the range are affected by the command. The slash mark is required.
/ *channel*	**A single DSP channel or the first DSP channel in a range.** The **second occurrence of this argument specifies either a single DSP channel or the last DSP channel in a range.** The slash mark is required.
statistics	Displays DSP statistics for a specific channel or range of channels.
slot-number	A single slot or the first slot in a range. To specify a range of slots, you can enter a **second slot in the syntax of this argument. The second slot specifies the end of the range.** All slots in the range are affected by the command.
traffic	Displays traffic on a specific channel or range of channels.

Command Modes

User EXEC (>)
Privileged EXEC (#)

Command History

Release	Modification
12.4(4)XC	The command was introduced on the Cisco AS5350XM and Cisco AS5400XM platforms.
12.4(11)T	The command was modified. Command output was enhanced to display information about DSP H.320 channels.

Usage Guidelines

Use this command when abnormal behavior occurs in the DSP voice channels. The channel or channels should have an active voice call at the time the command is executed.

Examples

The following is sample output from the **show voice dsp channel operational-status**command on slot 3/13/1:

```
Router# show voice dsp channel operational-status 3/13/1
 Operational status of Slot/DSP/Channel : 3/13/1
 Servicetype  : VOICE
 Codec Type  : gsmamr-nb
 Encapsulation : RTP
 Transmitted Packets : 346
 Transmitted Bytes : 11740
 Received Packets : 411
 Received Bytes : 11142
 Playout de-jitter mode :  None
 Playout de-jitter buffer minimum delay : 0 msec
 Playout de-jitter buffer initial delay : 0 msec
 Playout de-jitter buffer maximum delay : 0 msec
 Noise level : -5.0
 ERLLevel : 6
 ACOMLevel : 6
CodecPktPeriod=20 Milliseconds
CodecFrameFormat=bandwidth-efficient
CodecCrc=Disabled
CodecModes=3,6
CodecEncodeRate=6
CodecDecodeRate=6
CodecEncodeChanges=1
CodecDecodeChanges=0
CodecCrcFails=0
CodecBadFrameQuality=0
CodecInvalidCMRs=0
CodecInvalidFrameType=0
 Voice activity detection : Enabled
 Dtmf Relay : inband-voice
 ComfortNoisePak : 52
 TxVoiceDuration : 11560
 VoiceRxDuration : 3380
 Rx OutOfSeq Paks : 0
 Rx Late Paks : 0
 Rx Early Paks : 0
 Lost Packets : 0
 Playout Delay Current : 50
 Playout Delay Min : 50
 Playout Delay Max : 50
 Playout Delay ClockOffset : 80
 Playout Delay Jitter : 0
 Error Rx Drop : 0
 Error Tx Drop : 0
 Error Tx Control : 0
 Error Rx Control : 0
 Playout Error Predictive : 0
 Playout Error Interpolative : 0
 Playout Error Silence : 0
 Playout Error BufferOverFlow : 0
 Playout Error Retroactive : 0
 Playout Error Talkspurt : 0
```

The table below describes the significant fields shown in the display.

Table 186: show voice dsp channel Field Descriptions

Field	Description
DSP	Number of the DSP.
Channel	Number of the channel and its status.

Field	Description
Codec Type	Complexity setting.
TxVoiceDuration	Transmitted voice duration.

Related Commands

Command	Description
show voice dsp	Displays the current status or selective statistics of DSP voice channels,.

show voice dsp crash-dump

To display voice digital signal processor (DSP) crash dump information, use the show **voice dsp crash-dump**command in privileged EXEC configuration mode.

show voice dsp crash-dump

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.3(4)T	This command was introduced.

Examples

The following example checks your configuration:

```
Router# show voice dsp crash-dump
Voice DSP Crash-dump status:
    Destination file url is slot0:banjo-152-s
    File limit is 20
    Last DSP dump file written was
          tftp://112.29.248.12/tester/26-152-t2
    Next DSP dump file written will be slot0:banjo-152-s1
```

The following example shows that the crash dump feature is enabled:

```
Router# show voice dsp crash-dump
Voice DSP Crash-dump status:
    Destination file url is
          tftp://172.29.248.12/xxtir/dspdump6.bin
    File limit is 10
    Last DSP dump file written was
          tftp://172.29.248.12/xxtir/dspdump6.bin1
    Next DSP dump file written will be
          tftp://172.29.248.12/xxtir/dspdump6.bin2
```

The following example shows that the crash dump feature is disabled:

```
Router# show voice dsp crash-dump
Voice DSP Crash-dump status:
    Destination file url is
          tftp://172.29.248.12/xxtir/dspdump6.bin
    File limit is 0
    Last DSP dump file written was
          tftp://172.29.248.12/xxtir/dspdump6.bin1
DSP crash dump is currently disabled
To enable DSP crash dump, set file-limit to a non-zero number
```

Field descriptions should be self-explanatory.

Related Commands

Command	Description
debug voice dsp crash-dump	Displays crash dump debug information.
voice dsp crash-dump	Enables the crash dump feature and specifies the destination file and the file limit.

show voice dsp summary

To display the digital signal processor (DSP) summary, use the **show voice dsp summary**command in user EXEC or privileged EXEC mode.

show voice dsp summary [*slot* | *slot*/*dsp*] [*slot* | *slot*/*dsp*]

Syntax Description

slot	(Optional) A single slot or the first slot in a range. To specify a range of slots, you can enter a **second slot in the syntax of this argument. The second slot specifies the end of the range.** All slots in the range are affected by the command.
/ *dsp*	(Optional) A single DSP on the slot or the first DSP in a range. To specify a range of DSPs, you can enter a **second DSP in the syntax of this argument. The second DSP specifies the end of the range.** All DSPs in the range are affected by the command. The slash mark is required.

Command Modes

User EXEC (>)
Privileged EXEC (#)

Command History

Release	Modification
12.4(4)XC	This command was introduced. The command was implemented on the Cisco AS5350XM and Cisco AS5400XM platforms.
12.4(11)T	The command was modified. Command output was enhanced to display information about DSP H.320 channels.
12.4(19)	The command was modified. Command output was modified to accurately show the "Codectype" as "voice" rather than "fax" for T.38 calls.
12.4(18a)	The command was modified. Command output was modified to accurately show the "Codectype" as "voice" rather than "fax" for T.38 calls.
12.4(13f)	The command was modified. Command output was modified to accurately show the "Codectype" as "voice" rather than "fax" for T.38 calls.
12.4(15)T5	The command was modified. Command output was modified to accurately show the "Codectype" as "voice" rather than "fax" for T.38 calls.

Examples

The following sample output from the **show voice dsp summary** command shows summary information about DSPs:

```
Router# show voice dsp summary
Total number of DSPs = 48

Codectype       Calls    Codectype       Calls    Codectype       Calls
g729r8 pre-ietf     0    g729ar8             0    g726r16             0
g726r24             0    g726r32             0    g711ulaw            0
g711alaw            1    g728                0    g723r63             0
g723r53             0    gsmfr               0    gsmefr              0
```

```
g729br8             0    g729abr8            0    g723ar63            0
g723ar53            0    g729r8              0    t38                 0
clear-channel       0    vofr cisco          0    llcc                0
g726r40             0    transparent         0    modem-relay         0
cisco               0                        0                        0
pass-through        0    gsmamr-nb           0

Legend       :
======
Channel state: (s)shutdown   (a)active call (d)download pending
               (b)busiedout  (B)bad         (p)busyout pending
Call type    : (v)voice      (f)fax-relay   (_)not in use

Summary      :
=======
Channels     :  Total 768  In-Use    001
Calls        :  Total 001  Voice     001  Fax  000
             :  Free  713  Disabled  000

      DSP      DSP        DSP    Channel            Call
DSP#  State    Complexity Resets State              Type
2/1   ACTIVE   FLEXI      0      ________ ________   ________ ________
2/2   ACTIVE   FLEXI      0      ________ ________   ________ ________
2/3   ACTIVE   FLEXI      0      ________ ________   ________ ________
2/4   ACTIVE   FLEXI      0      ________ ________   ________ ________
2/5   ACTIVE   FLEXI      0      ________ ________   ________ ________
2/6   ACTIVE   FLEXI      0      ________ ________   ________ _________
```

The table below describes the significant fields shown in the display.

Table 187: show voice dsp summary Field Descriptions

Field	Description
DSP	Number of the DSP.
Codectype	Complexity setting.
Channels	Number of the channel and its status.
State	Status of the calls.

Related Commands

Command	Description
show voice dsp	Displays the current status or selective statistics of DSP voice channels,.

show voice eddri prefix

To show applicable prefixes for the event dispatcher and data repository interface (EDDRI), use the show voice eddri prefix command in privileged EXEC mode.

show voice eddri prefix [**prefix_number**]

Syntax Description

all	All neighbors
prefix_number	(Optional) Specified EDDRI prefix.

Command Default

No default behavior or values.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.3(1)	This command was introduced.

Usage Guidelines

If no prefix is specified, all configured prefixes appear.

The EDDRI notifies threaded grep (TGREP) when an attribute changes on some subsystems. EDDRI interacts with the dial-peer subsystem, trunk-group subsystems, call-control API (CCAPI) subsystem, and customer-relationship-management (CRM) subsystem to notify changes in particular attributes. EDDRI is responsible for creating the prefix database.

Examples

The following example shows output for the show voice eddri prefix command:

```
prefix 4 address family decimal
advertise flag 0x27 ac 24 tc 24 capacity timer 25 sec
AC_avg 24, FD_avg 0, SD_avg 0
succ_curr 0 tot_curr 0
succ_report 0 tot_report 0
changed 0 replacement position 0
trunk group castg2
dial peer tag 1001
```

Field descriptions should be self-explanatory.

Related Commands

Command	Description
debug voip eddri	Turns on debugging for the EDDRI.

show voice emergency locations

To display the emergency response locations (ERL) for E911 services, use **show voice emergency locations** command in privileged EXEC mode.

show voice emergency locations

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
IOS XE Fuji Release 16.8.1	This command was introduced.

Usage Guidelines

Use this command to display an ERL that identifies an area where emergency teams can quickly locate a 911 caller. This command displays ERL assignment by zone, device, and interfaces.

Examples

The following example displays ERL assignment by zone, device, and interfaces.

```
Router# show voice emergency locations
ERL ASSIGNMENT BY ZONE
DIAL-PEER   ZONE
=================
911         10

ERL ASSIGNMENT BY DEVICE AND INTERFACES
ERL         DEVICE
======================
12          dial-peer 100
```

Related Commands

voice emergency response	Configures emergency response location, zone, and settings for E911 services.

show voice enum-match-table

To display the rules of an ENUM match table, use the **show voice enum-match-table** command in privileged EXEC mode.

show voice enum-match-table [*table-number* [**sort**]]

Syntax Description

table -number	(Optional) ENUM match table to display, by number. Range is from 1 to 15.
sort	(Optional) Sorts the output by ascending table number.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.2(11)T	This command was introduced.

Usage Guidelines

This command displays the ENUM match table rules in the order in which they were defined. The sort keyword changes the display to list the rules from lowest to highest preference.

Examples

The following sample output displays the rules of ENUM match table number 3:

```
Router# show voice enum-match-table 3
voice enum_match_table 3
rule 1 5 /^9\(1.*\)/ /+\1/ cisco
rule 2 4 /^9011\(.*\)/ /+1408\1/ arpa
rule 10 1 /^(.*)/ /\1/ e164.cisco.com
```

The following sample output displays the ENUM match tables in ascending order by table number:

```
Router# show voice enum-match-table
voice enum-match-table 3
rule 1 5 /^9\(1.*\)/ /+\1/ cisco
rule 2 4 /^9011\(.*\)/ /+1408\1/ arpa
rule 10 1 /^(.*)/ /\1/ e164.cisco.com
voice enum-match-table 5
rule 2 4 /^9011\(.*\)/ /+1408\1/ arpa
rule 10 1 /^(.*)/ /\1/ e164.cisco.com
```

Field descriptions should be self-explanatory.

Related Commands

Command	Description
rule (ENUM configuration)	Defines the ENUM rule.
test enum	Tests the ENUM rule.
voice enum-match-table	Initiates the voice ENUM match table definition.

show voice hpi capture

To display capture status and statistics, use the **show voice hpi capture** command in privileged EXEC mode.

show voice hpi capture

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.2(10)	This command was introduced.
12.2(11)T	This command was integrated into Cisco IOS Release 12.2(11)T.

Usage Guidelines

This command displays the capture status and statistics. Use this command to confirm logger status and to examine the logger status output when the logger is running.

Caution Using the message logger feature in a production network environment increases CPU and memory usage on the gateway.

Note If you are experiencing problems with certain voice calls, the engineering team at Cisco might ask you to capture the control messages using the voice DSP logger. You can capture these messages by turning on the logger, repeating the problematic calls, and capturing the logs. Only Cisco engineers can determine if you should send the logs in for further review.

Examples

The following sample output shows capture statistics (HPI capture and logging) and status:

```
Router# show voice hpi capture
HPI Capture is on and is logging to URL ftp://172.23.184.216/d:\test_data.dat1 messages
sent to URL, 0 messages droppedMessage Buffer (total:inuse:free)  2134:0000:2134Buffer
Memory:699952 bytes, Message size:328 bytes
```

Field descriptions should be self-explanatory.

Related Commands

Command	Description
debug hpi	Enables debugging for HPI message events.
voice hpi capture	Allocates the Host Port Interface (HPI) capture buffer (size in bytes) and sets up or changes the destination URL for captured data.

show voice iec description

To display Internal Error Code (IEC) descriptions, use the show voice iec description command in user EXEC mode.

show voice iec description string

Syntax Description

string	Six-part dotted decimal string that displays the definition of an internal error code.

Command Default

No default behavior or values.

Command Modes

User EXEC

Command History

Release	Modification
12.3(4)T	This command was introduced.

Examples

The following example displays IEC descriptions:

```
Router# show voice iec description 1.1.180.2.21.4
IEC Version: 1
Entity: 1 (Gateway)
Category: 180 (Software error)
Subsystem: 2 (TCL IVR)
Error: 21 (Script syntax)
Diagnostic Code: 4
```

The table below describes significant fields shown in the display.

Table 188: show voice iec description Field Descriptions

Field	Description
IEC version	IEC version. A value of 1 indicates the Cisco IOS Release 12.3(4)T version.
Entity	Network physical entity (hardware system) that generated the IEC. The value 1 is assigned to the gateway.
Category	Error category, defined in terms of ITU-based Q.850 cause codes and VoIP network errors.
Subsystem	Specific subsystem within the physical entity where the IEC was generated.
Error Code	Error code within the subsystem.
Diagnostic Code	Cisco internal diagnostic value. Report this value to Cisco Technical Support.

Related Commands

Command	Description
show voice statistics iec	Displays IEC statistics.

show voice lmr

To display the Land Mobile Radio (LMR) related dynamic information and static information for LMR ports or a DS0 group, use the **show voice lmr** command in privileged EXEC mode.

show voice lmr [*slot/subunit/port* | *slot/port*:*ds0-group*] [**details** | **timing** [**warnings**]]

Syntax Description

slot/subunit/port	(Optional) Voice port that you specify with the *slot*/*subunit*/*port* designation. • *slot* specifies a router slot in which a voice network module (NM) is installed. Valid entries are router slot numbers for the particular platform. • *subunit* specifies a voice interface card (VIC) in which the voice port is located. Valid entries are 0 and 1. • *port* specifies an analog voice port number. Valid entries are 0 and 1. The slash marks are required.
slot/port **:** *ds0 -group*	(Optional) Voice port that you specify with the *slot*/*port* **:** *ds0-group*designation. • *slot* specifies a router slot in which the packet voice NM is installed. Valid entries are router slot numbers for the particular platform. • *port* specifies a T1 or E1 physical port in the voice WAN interface card (VWIC). Valid entries are 0 and 1. • *ds0 -group* specifies a T1 or E1 logical port number. T1 range is from 0 to 23. E1 range is from 0 to 30. The colon is required.
details	(Optional) Displays more information. If this keyword is omitted, less information is displayed.
timing	(Optional) Displays the timing configuration for all LMR ports.
warnings	(Optional) Displays all LMR ports that are having suspicious timing configuration.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.3(4)XD	This command was introduced.
12.3(7)T	This command was integrated into Cisco IOS Release 12.3(7)T.
12.4(24)T	This command was modified in a release earlier than Cisco IOS Release 12.4(24)T. The **timing** and **warnings** keywords were added.

Usage Guidelines

This command displays information for LMR voice ports only. If no voice port is specified, the command displays information for all ear and mouth (E&M) LMR voice ports.

When the **details** keyword is used, thiscommand displays information about timeouts, timers, and injected tones and pauses, in addition to detailed voice port and active call information found in the **show voice port** and **show call active voice** commands.

Examples

The following is sample output from the **show voice lmr** command for an E&M LMR analog voice port on a Cisco 3745 router:

```
Router# show voice lmr 2/0/0
2/0/0
=========
 Connection type: n/a
 Out Attenuation = 0 db, In Gain = 0 dB
 E-lead capability is inactive, polarity = normal
 M-lead capability is inactive, polarity = normal
 voice-class tone-signal test
 state = LMR_CONNECT, e-lead = off, m-lead = off
 full duplex, voice path = rx
 Terminating side of the connection
 TransmitPackets=113, TransmitBytes=2241
 ReceivePackets=113, ReceiveBytes=2241
 CoderTypeRate=g729r8
 NoiseLevel=-65, ACOMLevel=22
 OutSignalLevel=-68, InSignalLevel=-79
 RemoteIPAddress=10.5.25.40, RemoteUDPPort=17272
 Remote SignallingIPAddress=10.5.25.40, Port=15418
 Remote MediaIPAddress=10.5.25.40, Port=17272
 RoundTripDelay=2 ms
 SessionProtocol=cisco
 VAD =enabled
```

The following is sample output from the **show voice lmr details** command for an E&M LMR analog voice port on a Cisco 3745 router:

```
Router# show voice lmr 2/0/0 details
2/0/0
=========
 Description:
 Connection type: n/a
 Out Attenuation = 0 db, In Gain = 0 dB
 Timing hangover: 500 ms
 E-lead capability is inactive, polarity = normal
 M-lead capability is inactive, polarity = normal
 Timing hookflash-in: 480
 Timing delay-voice: 470 ms
 Music On Hold Threshold: -38 dB, Noise Threshold: -62 dB
 E&M type: 1, Operation:  2-wire
 Impedance is set to 600r Ohm
 lmr tear down timeout is set to 1800 second
 lmr PTT transmit timeout is not set
 lmr PTT receive timeout is not set
 voice-class tone-signal test
         inject tone 1 1950 3 150
         inject tone 2 2000 0 60
         inject pause 3 60
         inject tone 4 2175 3 150
         inject tone 5 1000 0 50
         inject guard-tone 6 1950 -10
```

```
state = LMR_CONNECT, e-lead = off, m-lead = off
full duplex, voice path = rx
Terminating side of the connection
TransmitPackets=113, TransmitBytes=2241
ReceivePackets=113, ReceiveBytes=2241
CoderTypeRate=g729r8
NoiseLevel=-66, ACOMLevel=22
OutSignalLevel=-68, InSignalLevel=-79
PeerAddress=37200
PeerSubAddress=
PeerId=200
SessionTarget=
RemoteIPAddress=10.5.25.40, RemoteUDPPort=17272
Remote SignallingIPAddress=10.5.25.40, Port=15418
Remote MediaIPAddress=10.5.25.40, Port=17272
RoundTripDelay=0 ms
SessionProtocol=cisco
VAD =enabled
SelectedQoS=best-effort
ProtocolCallId=
SessionTarget=
```

The table below describes the significant fields shown in the output, in the order in which they appear.

Table 189: show voice lmr Field Descriptions

Field	Description
Connection type	Type of connection between LMR routers: private line, automatic ringdown (PLAR), trunk, or n/a
Out Attenuation	Output attenuation.
In Gain	Input gain.
E-lead capability	Active or inactive.
polarity	Polarity of the E&M voice port: normal or reverse.
M-lead capability	Active or inactive.
voice class tone-signal	Name of the tone-signal voice class.
state=	Signaling state.
e-lead =	On or off.
m-lead =	On or off.
full duplex	Voice path for the voice port is operating in full duplex mode.
half duplex	Voice path for the voice port is operating in half duplex mode.
voice path	Transmit or receive.
TransmitPackets	Number of packets sent by this peer during this call.
TransmitBytes	Number of bytes sent by this peer during this call.

Field	Description
ReceivePackets	Number of packets received by this peer during this call.
ReceiveBytes	Number of bytes received by the peer during this call.
CoderTypeRate	Negotiated coder rate. This value specifies the send rate of voice or fax compression to its associated call leg for this call.
NoiseLevel	Active noise level for this call.
ACOMLevel	Current ACOM level for this call. ACOM is the combined loss achieved by the echo canceller, which is the sum of the Echo Return Loss, Echo Return Loss Enhancement, and nonlinear processing loss for the call.
OutSignalLevel	Active output signal level to the telephony interface used by this call.
InSignalLevel	Active input signal level from the telephony interface used by this call.
RemoteIPAddress	Remote system IP address for the VoIP call.
RemoteUDPPort	Remote system User Datagram Protocol (UDP) listener port to which voice packets are sent.
Remote SignallingIPAddress, Port	Call control server IP address and signaling port number.
Remote MediaIPAddress, Port	Remote side media server IP address and RTP port number.
RoundTripDelay	Voice packet round trip delay between the local and remote systems on the IP backbone for this call.
SessionProtocol	Session protocol used for an Internet call between the local and remote routers through the IP backbone.
VAD	Whether voice activation detection (VAD) is enabled.
Description	Description of what the port is connected to.
Timing hangover	Number of milliseconds of delay before the digital signal processor (DSP) tells Cisco IOS software to turn off the E-lead after the DSP detects that the voice stream has stopped.
Timing hookflash-in	Maximum duration of a hookflash for a Foreign Exchange Station (FXS) interface.
Timing delay-voice	Delay before a voice packet is played out.
Music On Hold Threshold	Decibel level of music played when calls are put on hold.
Noise Threshold	Noise threshold for incoming calls.
E&M type	E&M signaling type.
Operation	2-wire or 4-wire operation.
Impedance	Terminating impedance of the interface.

Field	Description
lmr tear down timeout	Time for which the voice port waits before tearing down an LMR connection after detecting no voice activity.
lmr PTT transmit timeout	Maximum time for transmitting a voice packet.
lmr PTT receive timeout	Maximum time for receiving a voice packet.
inject pause	Pause injected before the voice packet is played out.
inject tone	Tone injected before the voice packet is played out.
inject guard-tone	Guard tone played out with the voice packet.
PeerAddress	Destination pattern or number associated with this peer.
PeerSubAddress	Subaddress when this call is connected.
PeerId	ID value of the peer table entry to which this call was made.
SessionTarget	Network-specific address to receive calls from the dial peer.
SelectedQoS	Selected RSVP quality of service (QoS) for this call.
ProtocolCallId	Voice signaling specific call ID.

Related Commands

Command	Description
show call active voice	Displays call information for voice calls in progress.
show voice port	Displays configuration information about a specific voice port.

show voice pcm capture

To display PCM capture status and statistics, use the **show voice pcm capture** command in privileged EXEC mode.

show voice pcm capture

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
15.2(2)T	This command was introduced.

Usage Guidelines

This command displays the PCM capture status and statistics. Use this command to confirm logger status and to examine the logger status output when the logger is running.

Examples

The following is sample output from the **show voice pcm capture** command :

```
Router# show voice pcm capture
PCM Capture is on and is logging to URL tftp://10.10.1.2/acphan/
50198 messages sent to URL, 0 messages dropped
Message Buffer (total:inuse:free) 200000:0:200000
Buffer Memory: 68000000 bytes, Message size: 340 bytes
```

Related Commands

Command	Description
voice pcm capture	Allocates the number of Pulse Code Modulation (PCM) capture buffers, sets up or changes the destination URL for captured data, enables PCM capture on-demand, and changes the PCM capture trigger string by the user.

show voice port

To display configuration information about a specific voice port, use the **show voice port** command in privileged EXEC mode.

Cisco 1750 Router
show voice port *slot/port*

Cisco 2600 and Cisco 3600 Series Router with Analog Voice Ports
show voice port [*slot/subunit/port* | **summary**]

Cisco 2600 and Cisco 3600 Series Router with Digital Voice Ports (with T1 Packet Voice Trunk Network Modules)
show voice port [*slot/port***:***ds0-group* | **summary**]

Cisco AS5300 Universal Access Server
show voice port *controller-number***:D**

Cisco 7200 Series Router
show voice port {*slot/port***:***ds0-group-number* | *slot/subunit/port*}

Syntax Description

Cisco 1750 Router	
slot	Slot number in the router in which the VIC is installed. Valid entries are 0, 1, and 2, depending on the slot in which it is installed.
/ *port*	Voice port. Valid entries are 0 and 1. The slash mark is required.
Cisco 2600 and Cisco 3600 Series Router with Analog Voice Ports	
slot / *subunit* / *port*	(Optional) The analog voice port designation: • *slot* -- Router slot in which a voice network module (VNM) is installed. Valid entries are router slot numbers for the particular platform. • *subunit* --Voice Interface Card (VIC) in which the voice port is located. Valid entries are 0 and 1. (The VIC fits into the voice network module.) The slash mark is required. • *port*-- Analog voice port number. Valid entries are 0 and 1. The slash mark is required.
summary	(Optional) Displays a summary of all voice ports.
Cisco 2600 and Cisco 3600 Series Router with Digital Voice Ports	

Cisco 1750 Router	
slot / *port* **:** *ds0 -group*	(Optional) Specifies the digital voice port designation: • *slot*-- Router slot in which the packet voice trunk network module (NM) is installed. Valid entries are router slot numbers for the particular platform. • / *port*-- T1 or E1 physical port in the voice WAN interface card (VWIC). Valid entries are 0 and 1. (One VWIC fits in an NM.) The slash mark is required. • **:** *ds0 -group*--T1 or E1 logical port number. T1 range is 0 to 23. E1 range is 0 to 30. The colon is required.
summary	(Optional) Displays a summary of all voice ports.
Cisco AS5300 Universal Access Server	
controller -number	T1 or E1 controller.
:D	D channel that is associated with the ISDN PRI. The colon is required.
Cisco 7200 Series Router	
slot	Router location where the voice port adapter is installed. Range is 0 to 3.
/ *port*	Voice interface card location. Valid entries are 0 and 1. The slash mark is required.
: *ds0-group-number*	Defined DS0 group number. Because each defined DS0 group number is represented on a separate voice port, you can define individual DS0s on the digital T1/E1 card. The colon is required.
slot	Slot number in the Cisco router where the VIC is installed. Range is 0 to 3, depending on the slot where it is installed.
/ *subunit*	Subunit on the VIC where the voice port is located. Valid entries are 0 and 1. The slash mark is required.
/ *port*	Voice port number. Valid entries are 0 and 1. The slash mark is required.

Command Modes

Privileged EXEC

Command History

Release	Modification
11.3(1)T	This command was introduced on the Cisco 3600 series.
11.3(1)MA	This command was modified. Port-specific values for the Cisco MC3810 were added.
12.0(3)T	This command was modified. Port-specific values for the Cisco MC3810 were added.

Release	Modification
12.0(5)XK	This command was modified. The *ds0-group* argument was added for the Cisco 2600 series and Cisco 3600 series.
12.0(5)XE	This command was modified. Additional syntax was created for digital voice to allow specification of the DS0 group. This command applies to VoIP on the Cisco 7200 series.
12.0(7)T	This command was integrated into Cisco IOS Release 12.0(7)T.
12.0(7)XK	This command was modified. The **summary** keyword was added for the Cisco 2600 series and Cisco 3600 series. The*ds0-group* argument was added for the Cisco MC3810.
12.1(2)T	This command was integrated into Cisco IOS Release 12.1(2)T.
12.2(8)T	This command was modified. This command was implemented for direct inward dial (DID) on the Cisco IAD2420 series.
12.2(2)XN	This command was modified. Support for enhanced Media Gateway Control Protocol (MGCP) voice gateway interoperability was added to Cisco CallManager Version 3.1 for the Cisco 2600 series, Cisco 3600 series, and Cisco Gateway 200 (Cisco VG200).
12.2(11)T	This command was integrated into Cisco IOS Release 12.2(11)T and Cisco CallManager Version 3.2. It was implemented on the Cisco IAD2420 series.
12.4(11)T	This command was modified. This command was enhanced to display voice class called-number-pool configuration information for the voice port.
12.4(12)	This command was modified. This command was integrated into Cisco IOS Release 12.4(12) and output was modified to display the parameter set by the **timing sup-disconnect** command.
15.0(1)XA	This command was modified. The output was enhanced to display the logical partitioning class of restriction (LPCOR) policy for incoming and outgoing calls.
15.1(1)T	This command was integrated into Cisco IOS Release 15.1(1)T.
15.1(3)T	This command was modified. The output of this command was enhanced to display the connection status of foreign exchange office (FXO) ports.

Usage Guidelines

Use this command to display configuration and VIC-specific information about a specific port.

This command works on Voice over IP, Voice over Frame Relay, and Voice over ATM.

The **ds0-group** command automatically creates a logical voice port that is numbered as follows on Cisco 2600, Cisco 3600 series, and Cisco 7200 series routers: *slot* **/** *port* **:** *ds0-group-number*. Although only one voice port is created for each group, applicable calls are routed to any channel in the group.

Note This command is not supported on Cisco AS5350, Cisco AS5400, Cisco AS5800, and Cisco AS5850 platforms for Non-Facility Associated Signaling (NFAS) configuration.

Examples

The following is sample output from the **show voice port** command for an E&M analog voice port:

```
Router# show voice port 1/0/0
E&M Slot is 1, Sub-unit is 0, Port is 0
 Type of VoicePort is E&M
 Operation State is unknown
 Administrative State is unknown
 The Interface Down Failure Cause is 0
 Alias is NULL
 Noise Regeneration is disabled
 Non Linear Processing is disabled
 Music On Hold Threshold is Set to 0 dBm
 In Gain is Set to 0 dB
 Out Attenuation is Set to 0 dB
 Echo Cancellation is disabled
 Echo Cancel Coverage is set to 16ms
 Connection Mode is Normal
 Connection Number is not set
 Initial Time Out is set to 0 s
 Interdigit Time Out is set to 0 s
 Analog Info Follows:
 Region Tone is set for northamerica
 Currently processing none
 Maintenance Mode Set to None (not in mtc mode)
 Number of signaling protocol errors are 0
 Voice card specific Info Follows:
 Signal Type is wink-start
 Operation Type is 2-wire
 Impedance is set to 600r Ohm
 E&M Type is unknown
 Dial Type is dtmf
 In Seizure is inactive
 Out Seizure is inactive
 Digit Duration Timing is set to 0 ms
 InterDigit Duration Timing is set to 0 ms
 Pulse Rate Timing is set to 0 pulses/second
 InterDigit Pulse Duration Timing is set to 0 ms
 Clear Wait Duration Timing is set to 0 ms
 Wink Wait Duration Timing is set to 0 ms
 Wink Duration Timing is set to 0 ms
 Delay Start Timing is set to 0 ms
 Delay Duration Timing is set to 0 ms
```

The following is sample output from the **show voice port** command for an E&M digital voice port:

```
Router# show voice port 1/0/1
receEive and transMit Slot is 1, Sub-unit is 0, Port is 1
 Type of VoicePort is E&M
 Operation State is DORMANT
 Administrative State is UP
 No Interface Down Failure
 Description is not set
 Noise Regeneration is enabled
 Non Linear Processing is enabled
 Music On Hold Threshold is Set to -38 dBm
 In Gain is Set to 0 dB
 Out Attenuation is Set to 0 dB
 Echo Cancellation is enabled
 Echo Cancel Coverage is set to 8 ms
 Connection Mode is normal
 Connection Number is not set
 Initial Time Out is set to 10 s
 Interdigit Time Out is set to 10 s
 Region Tone is set for US
```

The following is sample output from the **show voice port** command for a foreign exchange station (FXS) analog voice port:

```
Router# show voice port 1/1/1
Foreign Exchange Station 1/1/1 Slot is 1, Sub-unit is 1, Port is 1
 Type of VoicePort is FXS  VIC2-2FXS
 Operation State is DORMANT
 Administrative State is UP
 The Last Interface Down Failure Cause is Administrative Shutdown
 Description is I am a FXS LoopStart port
 Noise Regeneration is enabled
 Non Linear Processing is enabled
 Non Linear Mute is disabled
 Non Linear Threshold is -21 dB
 Music On Hold Threshold is Set to -38 dBm
 In Gain is Set to 0 dB
 Out Attenuation is Set to 3 dB
 Echo Cancellation is enabled
 Echo Cancellation NLP mute is disabled
 Echo Cancellation NLP threshold is -21 dB
 Echo Cancel Coverage is set to 64 ms
 Echo Cancel worst case ERL is set to 6 dB
 Playout-delay Mode is set to adaptive
 Playout-delay Nominal is set to 60 ms
 Playout-delay Maximum is set to 250 ms
 Playout-delay Minimum mode is set to default, value 40 ms
 Playout-delay Fax is set to 300 ms
 Connection Mode is normal
 Connection Number is not set
 Initial Time Out is set to 10 s
 Interdigit Time Out is set to 10 s
 Call Disconnect Time Out is set to 60 s
 Supervisory Disconnect Time Out is set to 750 ms
 Ringing Time Out is set to 180 s
 Wait Release Time Out is set to 30 s
 Companding Type is u-law
 Region Tone is set for US
 Analog Info Follows:
 Currently processing none
 Maintenance Mode Set to None (not in mtc mode)
 Number of signaling protocol errors are 0
 Impedance is set to 600r Ohm
 Station name None, Station number None
 Translation profile (Incoming):
 Translation profile (Outgoing):
 lpcor (Incoming): local_group
 lpcor (Outgoing): local_group
 Voice card specific Info Follows:
 Signal Type is loopStart
 Ring Frequency is 25 Hz
 Hook Status is On Hook
 Ring Active Status is inactive
 Ring Ground Status is inactive
 Tip Ground Status is active
 Digit Duration Timing is set to 100 ms
 InterDigit Duration Timing is set to 100 ms
 Hookflash-in Timing is set to max=1000 ms, min=150 ms
 Hookflash-out Timing is set to 400 ms
 No disconnect acknowledge
 Ring Cadence is defined by CPTone Selection
 Ring Cadence are [20 40] * 100 msec
 Ringer Equivalence Number is set to 1
```

The following is sample output from the **show voice port** command for an FXO analog voice port:

```
Router# show voice port 1/0/1
Foreign Exchange Office 1/0/1 Slot is 1, Sub-unit is 0, Port is 1
 Type of VoicePort is FXO
 Operation State is DORMANT
 Administrative State is UP
 The Last Interface Down Failure Cause is Administrative Shutdown
 Description is I am an FXO LoopStart port
 Noise Regeneration is enabled
 Non Linear Processing is enabled
 Non Linear Mute is disabled
 Non Linear Threshold is -21 dB
 Music On Hold Threshold is Set to -38 dBm
 In Gain is Set to 0 dB
 Out Attenuation is Set to 3 dB
 Echo Cancellation is enabled
 Echo Cancellation NLP mute is disabled
 Echo Cancellation NLP threshold is -21 dB
 Echo Cancel Coverage is set to 64 ms
 Echo Cancel worst case ERL is set to 6 dB
 Playout-delay Mode is set to adaptive
 Playout-delay Nominal is set to 60 ms
 Playout-delay Maximum is set to 250 ms
 Playout-delay Minimum mode is set to default, value 40 ms
 Playout-delay Fax is set to 300 ms
 Connection Mode is normal
 Connection Number is not set
 Initial Time Out is set to 10 s
 Interdigit Time Out is set to 10 s
 Call Disconnect Time Out is set to 60 s
 Ringing Time Out is set to 180 s
 Wait Release Time Out is set to 30 s
 Companding Type is u-law
 Region Tone is set for US
 Analog Info Follows:
 Currently processing none
 Maintenance Mode Set to None (not in mtc mode)
 Number of signaling protocol errors are 0
 Impedance is set to 600r Ohm
 Station name None, Station number None
 Translation profile (Incoming):
 Translation profile (Outgoing):
 Voice card specific Info Follows:
 Signal Type is loopStart
 Battery-Reversal is enabled
 Number Of Rings is set to 1
 Supervisory Disconnect is signal
 Answer Supervision is inactive
 Hook Status is On Hook
 Ring Detect Status is inactive
 Ring Ground Status is inactive
 Tip Ground Status is inactive
 Dial Out Type is dtmf
 Digit Duration Timing is set to 100 ms
 InterDigit Duration Timing is set to 100 ms
 Pulse Rate Timing is set to 10 pulses/second
 InterDigit Pulse Duration Timing is set to 750 ms
 Percent Break of Pulse is 60 percent
 GuardOut timer is 2000 ms
 Minimum ring duration timer is 125 ms
 Hookflash-in Timing is set to 600 ms
 Hookflash-out Timing is set to 400 ms
```

```
 Supervisory Disconnect Timing (loopStart only) is set to 750 ms
 OPX Ring Wait Timing is set to 6000 ms
```

The following is sample output from the **show voice port summary**command. Note that for the connected FXO analog voice port 0/2/0, which has the ADMIN state of "up" and the OPER state of "dorm," this output shows that the IN STATUS is "idle" and the OUT STATUS is "on-hook":

```
Router# show voice port summary
                                          IN       OUT
PORT            CH   SIG-TYPE   ADMIN OPER STATUS   STATUS   EC
=============== == ============ ===== ==== ======== ======== ==
0/0/0           --  fxs-ls      up    dorm on-hook  idle     y
0/0/1           --  fxs-ls      up    dorm on-hook  idle     y
0/3/0:23        01  isdn-voice  up    dorm none     none     y
0/3/0:23        02  isdn-voice  up    dorm none     none     y
.
.
.
0/1/0           --  did-in-wnk  up    dorm idle     idle     y
0/1/1           --  did-in-wnk  up    dorm idle     idle     y
0/2/0           --  fxo-ls      up    dorm idle     on-hook  y
0/2/1           --  fxo-ls      up    down idle     off-hook y
2/0/0           --  fxs-ls      up    dorm on-hook  idle     y
2/0/1           --  fxs-ls      up    dorm on-hook  idle     y
2/0/2           --  fxs-ls      up    dorm on-hook  idle     y
2/0/3           --  fxs-ls      up    dorm on-hook  idle     y
2/0/4           --  fxs-ls      up    dorm on-hook  idle     y
2/0/5           --  fxs-ls      up    dorm on-hook  idle     y
2/0/6           --  fxs-ls      up    dorm on-hook  idle     y
2/0/7           --  fxs-ls      up    dorm on-hook  idle     y
```

Note If the FXO port 0/2/0 is disconnected, the output of the **show voice port summary** command changes so that the OUT STATUS is reported as "off-hook," and the OPER state changes to "down."

The following is sample output from the **show voice port** command for an ISDN voice port:

```
Router# show voice port
ISDN 2/0:23 Slot is 2, Sub-unit is 0, Port is 23
 Type of VoicePort is ISDN-VOICE
 Operation State is DORMANT
 Administrative State is UP
 No Interface Down Failure
 Description is not set
 Noise Regeneration is enabled
 Non Linear Processing is enabled
 Non Linear Mute is disabled
 Non Linear Threshold is -21 dB
 Music On Hold Threshold is Set to -38 dBm
 In Gain is Set to 0 dB
 Out Attenuation is Set to 0 dB
 Echo Cancellation is enabled
 Echo Cancellation NLP mute is disabled
 Echo Cancellation NLP threshold is -21 dB
 Echo Cancel Coverage is set to 64 ms
 Echo Cancel worst case ERL is set to 6 dB
 Playout-delay Mode is set to adaptive
 Playout-delay Nominal is set to 60 ms
 Playout-delay Maximum is set to 250 ms
 Playout-delay Minimum mode is set to default, value 40 ms
```

```
 Playout-delay Fax is set to 300 ms
 Connection Mode is normal
 Connection Number is not set
 Initial Time Out is set to 10 s
 Interdigit Time Out is set to 10 s
 Call Disconnect Time Out is set to 60 s
 Ringing Time Out is set to 180 s
 Wait Release Time Out is set to 30 s
 Companding Type is u-law
 Region Tone is set for US
 Station name None, Station number None
 Translation profile (Incoming):
 Translation profile (Outgoing):
 Voice class called number pool:
DS0 channel specific status info:
                                        IN      OUT
    PORT       CH  SIG-TYPE    OPER STATUS    STATUS    TIP     RING
    2/0:23     01  isdn-voice  up   none      none
    2/0:23     02  isdn-voice  up   none      none
    2/0:23     03  isdn-voice  up   none      none
    2/0:23     04  isdn-voice  up   none      none
    2/0:23     05  isdn-voice  up   none      none
    2/0:23     06  isdn-voice  up   none      none
    2/0:23     07  isdn-voice  dorm none      none
    2/0:23     08  isdn-voice  dorm none      none
    2/0:23     09  isdn-voice  dorm none      none
    2/0:23     10  isdn-voice  dorm none      none
    2/0:23     11  isdn-voice  dorm none      none
    2/0:23     12  isdn-voice  dorm none      none
    2/0:23     13  isdn-voice  dorm none      none
    2/0:23     14  isdn-voice  dorm none      none
    2/0:23     15  isdn-voice  dorm none      none
    2/0:23     16  isdn-voice  dorm none      none
    2/0:23     17  isdn-voice  dorm none      none
    2/0:23     18  isdn-voice  dorm none      none
    2/0:23     19  isdn-voice  dorm none      none
    2/0:23     20  isdn-voice  dorm none      none
    2/0:23     21  isdn-voice  dorm none      none
    2/0:23     22  isdn-voice  dorm none      none
    2/0:23     23  isdn-voice  dorm none      none
```

The following is sample output from the **show voice port**command for the connected FXO analog voice port 0/2/0, which has the Administrative State of "UP" and the Operation State of "DORMANT":

```
Router# show voice port 0/2/0
Foreign Exchange Office 0/2/0 Slot is 0, Sub-unit is 2, Port is 0
 Type of VoicePort is FXO
 Operation State is DORMANT
 Administrative State is UP
 No Interface Down Failure
 Description is not set
 Noise Regeneration is enabled
 Non Linear Processing is enabled
 Non Linear Mute is disabled
 Non Linear Threshold is -21 dB
 Music On Hold Threshold is Set to -38 dBm
 In Gain is Set to 0 dB
 Out Attenuation is Set to 3 dB
 Echo Cancellation is enabled
 Echo Cancellation NLP mute is disabled
 Echo Cancellation NLP threshold is -21 dB
 Echo Cancel Coverage is set to 128 ms
 Echo Cancel worst case ERL is set to 6 dB
```

```
Playout-delay Mode is set to adaptive
Playout-delay Nominal is set to 60 ms
Playout-delay Maximum is set to 1000 ms
Playout-delay Minimum mode is set to default, value 40 ms
Playout-delay Fax is set to 300 ms
Connection Mode is normal
Connection Number is not set
Initial Time Out is set to 15 s
Interdigit Time Out is set to 10 s
Call Disconnect Time Out is set to 60 s
Power Denial Disconnect Time Out is set to 1000 ms
Ringing Time Out is set to 180 s
Wait Release Time Out is set to 30 s
Companding Type is u-law
Region Tone is set for US
Analog Info Follows:
Currently processing none
Maintenance Mode Set to None (not in mtc mode)
Number of signaling protocol errors are 0
Impedance is set to 600r Ohm
Station name None, Station number None
Translation profile (Incoming):
Translation profile (Outgoing):
lpcor (Incoming):
lpcor (Outgoing):
Voice card specific Info Follows:
Signal Type is loopStart
Battery-Reversal is enabled
Number Of Rings is set to 1
Supervisory Disconnect is signal
Answer Supervision is inactive
Hook Status is On Hook
Ring Detect Status is inactive
Ring Ground Status is inactive
Tip Ground Status is inactive
Dial Out Type is dtmf
Digit Duration Timing is set to 100 ms
InterDigit Duration Timing is set to 100 ms
Pulse Rate Timing is set to 10 pulses/second
InterDigit Pulse Duration Timing is set to 750 ms
Percent Break of Pulse is 60 percent
GuardOut timer is 2000 ms
Minimum ring duration timer is 125 ms
Hookflash-in Timing is set to 600 ms
Hookflash-out Timing is set to 400 ms
Supervisory Disconnect Timing (loopStart only) is set to 350 ms
OPX Ring Wait Timing is set to 6000 ms
Secondary dialtone is disabled
```

Note If the FXO port 0/2/0 is disconnected, the output of the **show voice port**command changes so that the Administrative State remains "UP" but the Operation State is "DOWN." Beginning in Cisco IOS Release 15.1(3)T, there is improved status monitoring of FXO ports--any time an FXO port is connected or disconnected, a message is displayed to indicate the status change. For example, the following message is displayed to report that a cable has been connected, and the status is changed to "up" for FXO port 0/2/0: 000118: Jul 14 18:06:05.122 EST: %LINK-3-UPDOWN: Interface Foreign Exchange Office 0/2/0, changed state to operational status up due to cable reconnection

The table below describes significant fields shown in these outputs, in alphabetical order.

Table 190: show voice port Field Descriptions

Field	Description
Administrative State	Administrative state of the voice port.
Alias	User-supplied alias for the voice port.
Clear Wait Duration Timing	Time (in milliseconds [ms]) of inactive seizure signal to declare call cleared.
Companding Type	Companding standard used to convert between analog and digital signals in pulse code modulation (PCM) systems.
Connection Mode	Connection mode of the interface.
Connection Number	Full E.164 telephone number used to establish a connection with the trunk or private line automatic ringdown (PLAR) mode.
Currently Processing	Type of call currently being processed: none, voice, or fax.
Delay Duration Timing	Maximum delay signal duration (in ms) for delay dial signaling.
Delay Start Timing	Timing (in ms) of generation of delayed start signal from detection of incoming seizure.
Dial Type	Out-dialing type of the voice port.
Digit Duration Timing	Dual-tone multifrequency (DTMF) digit duration (in ms).
E&M Type	Type of E&M interface.
Echo Cancel Coverage	Echo cancel coverage for this port.
Echo Cancellation	Whether echo cancellation is enabled for this port.
Impedance	Configured terminating impedance for the E&M interface.
In Gain	Amount of gain (in decibels [dB]) inserted at the receiver side of the interface.
In Seizure	Incoming seizure state of the E&M interface.
Initial Time Out	Amount of time (in seconds) the system waits for an initial input digit from the caller.
Interdigit Duration Timing	DTMF interdigit duration (in seconds).
InterDigit Pulse Duration Timing	Pulse dialing interdigit timing (in ms).
Interdigit Time Out	Amount of time (in seconds) the system waits for a subsequent input digit from the caller.
Lpcor (Incoming)	Setting of the **lpcor incoming** command.
Lpcor (Outgoing)	Setting of the **lpcor outgoing** command.

Field	Description
Maintenance Mode	Maintenance mode of the voice port.
Music On Hold Threshold	Configured music-on-hold threshold value for this interface.
Noise Regeneration	Whether background noise should be played to fill silent gaps if voice activity detection (VAD) is activated.
Non Linear Processing	Whether nonlinear processing is enabled for this port.
Number of signaling protocol errors	Number of signaling protocol errors.
Operation State	Operational state of the voice port.
Operation Type	Operation type of the E&M signal: 2-wire or 4-wire.
Out Attenuation	Amount of attenuation (in dB) inserted at the transmit side of the interface.
Out Seizure	Outgoing seizure state of the E&M interface.
Port	Port number for the interface associated with the voice interface card.
Pulse Rate Timing	Pulse dialing rate, in pulses per second (pps).
Region Tone	Configured regional tone for this interface.
Ring Active Status	Ring active indication.
Ring Cadence	Configured ring cadence for this interface.
Ring Frequency	Configured ring frequency (in hertz) for this interface.
Ring Ground Status	Ring ground indication.
Ringing Time Out	Ringing timeout duration (in seconds).
Signal Type	Type of signaling for a voice port: delay-dial, ground-start, immediate, loop-start, and wink-start.
Slot	Slot used in the voice interface card for this port.
Sub-unit	Subunit used in the voice interface card for this port.
Tip Ground Status	Tip ground indication.
Type of VoicePort	Type of voice port: FXO, FXS, or E&M.
The Interface Down Failure Cause	Text string describing why the interface is down,
Wait Release Time Out	Length of time (in seconds) that a voice port stays in call-failure state while a busy tone, reorder tone, or out-of-service tone is sent to the port.
Wink Duration Timing	Maximum wink duration (in ms) for wink-start signaling.

Field	Description
Wink Wait Duration Timing	Maximum wink wait duration (in ms) for wink-start signaling.

Related Commands

Command	Description
ds0 group	Specifies the DS0 time slots that make up a logical voice port on a T1 or E1 controller and specifies the signaling type by which the router communicates with the PBX or PSTN.
timing sup-disconnect	Defines the minimum time to ensure that an on-hook indication is intentional and not an electrical transient on the line before a supervisory disconnect occurs (based on power denial signaled by the PSTN or PBX).

show voice sip license

To display SIP trunk license information, use **show voice sip license** command in privileged EXEC mode.

show voice sip license [stats {table} | status]

Syntax Description

stats	Displays license usage over time.
table	(Optional) Displays license usage over time in tabular format.
status	Displays license status.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Amsterdam 17.2.1r	This command was introduced.
Cisco IOS XE Amsterdam 17.3.2 and Cisco IOS XE Bengaluru 17.4.1a	This command was modified to support Cisco Smart Licensing Using Policy.
Cisco IOS XE Bengaluru 17.6.1a	This command was modified to display licensing information for WebSockets in CUBE.

Usage Guidelines

Use **show voice sip license stats** command to display license usage in graphical format. The output includes eight graphs. Four graphs display "CUBE Standard Trunk License Usage" and four graphs display "TDM-SIP Trunk Sessions" details. The following describes how to interpret the graphical data:

- **License usage for the last 60 seconds**—The graph displays the licenses that are used in the last 60 seconds. X-axis represents the time in seconds and Y-axis represents the licenses that are used. # represents the licenses that are used.

  For example, in the following graph, 15 licenses were used at the second second.

```
                        1
     1122334455667788990998877665544332211
     5050505050505061505050505050505050505
100                   ###
 90                 #######
 80               ###########
 70             ###############
 60           ###################
 50         #######################
 40       ###########################
 30     #############################
 20    ##############################
 10  ##################################
   0....5....1....1....2....2....3....3....4....4....5....5....6
             0    5    0    5    0    5    0    5    0    5    0
      CUBE Standard Trunk License Usage (last 60 seconds)
```

- **License usage for the last 60 minutes**—The graph displays the licenses that are used in the last 60 minutes. X-axis represents the time in minutes and Y-axis represents the licenses that are used. The

values on the Y-axis vary based on the licenses used. **#** represents the average licenses used. ***** represents the maximum licenses used. The maximum licenses that are used over a minute are calculated by taking the average of top three values of licenses that are used over the 60 seconds in that minute.

For example, in the following graph, on the 48th minute, a maximum of 383 licenses were used.

```
                                                  369863146641
                                                 8880900440044
                                                 3330922440011
910                                                 **
820                                                 #*
730                                                 ##
640                                                *##*   **
550                                                ###*   ##
460                                                ####  *###*
370                                               *####  *###*
280                                               #####* ####
190                                               ###### ####
100                                              *######*####*
 10                                              ##############
   0....5....1....1....2....2....3....3....4....4....5....5....6
             0    5    0    5    0    5    0    5    0    5    0
        CUBE Standard Trunk License Usage (last 60 minutes)
        * = maximum     # = average
```

- **License usage for the last 72 hours**—The graph displays the licenses that are used in the last 72 hours. X-axis represents the time in hours and Y-axis represents the licenses that are used. The values on the Y-axis vary based on the licenses used. **#** represents the average licenses used. ***** represents the maximum licenses used. The maximum licenses that are used over each hour are the same as the maximum licenses used over the minutes in that hour. While computing license consumption over a period, the maximum value during that period is considered.

  For example, in the following graph, during the first hour, a maximum of 900 licenses were used.

```
    9
    0
    0
970
890 *
810 *
730 *
650 *
570 *
490 *
410 *
330 *
250 *
170 #
   0....5....1....1....2....2....3....3....4....4....5....5....6....6....7..
             0    5    0    5    0    5    0    5    0    5    0    5    0
        CUBE Standard Trunk License Usage (last 72 hours)
        * = maximum     # = average
```

- **License usage for the last 72 days**—The graph displays the licenses that are used for the last 72 days. X-axis represents the time in hours and Y-axis represents the licenses that are used. The values on the Y-axis vary based on the licenses used. **#** represents the average licenses used. ***** represents the maximum licenses used. The maximum licenses used each day is the same as the maximum licenses used over the

hours in that day. While computing license consumption over a period, the maximum value during that period is considered.

For example, in the following graph, on day 1, a maximum of 950 licenses were used.

```
     9 2
     5 0
     0 0
 1000 *
  900 *
  800 *
  700 *
  600 *
  500 *
  400 *
  300 *
  200 * *
  100 * *
    0....5....1....1....2....2....3....3....4....4....5....5....6....6....7..
              0    5    0    5    0    5    0    5    0    5    0    5    0
         CUBE Standard Trunk License Usage (last 72 days)
         * = maximum     # = average
```

The following is a sample TDM-SIP Trunk Sessions graph. **#** represents the average licenses used. ***** represents the maximum licenses used. In the below graph, a maximum of 1 TDM-SIP trunk session was used during the first hour.

```
   11
10
 9
 8
 7
 6
 5
 4
 3
 2
 1 **
  0....5....1....1....2....2....3....3....4....4....5....5....6....6....7..
            0    5    0    5    0    5    0    5    0    5    0    5    0
       TDM-SIP Trunk Sessions (last 72 hours)
       * = maximum   # = average
```

Use the **table** keyword to display the licenses used over time in tabular format. The output includes the following tables for "CUBE Standard Trunk License Usage" and "TDM-SIP Trunk Sessions":

- License usage for the last 60 seconds
- License usage for the last 60 minutes
- License usage for the last 72 hours
- License usage for the last 72 days

The license usage for WebSockets in CUBE is displayed in graphical format using **show voice sip license stats**. For display of the licensing usage information in tabular format, use **show voice sip license stats table**. License usage is displayed for Enhanced, Standard, and Aggregate call counts for WebSockets. TDM calls are not counted for WebSockets in CUBE.

Examples

The following are sample outputs for **show voice sip license stats** command:

```
cube#show voice sip license stats

          11:01:01 AM Thursday Aug 29 2019 IST




  10
   9
   8
   7
   6
   5
   4
   3
   2
   1
    0....5....1....1....2....2....3....3....4....4....5....5....6
              0    5    0    5    0    5    0    5    0    5    0
         CUBE Standard Trunk License Usage (last 60 seconds)

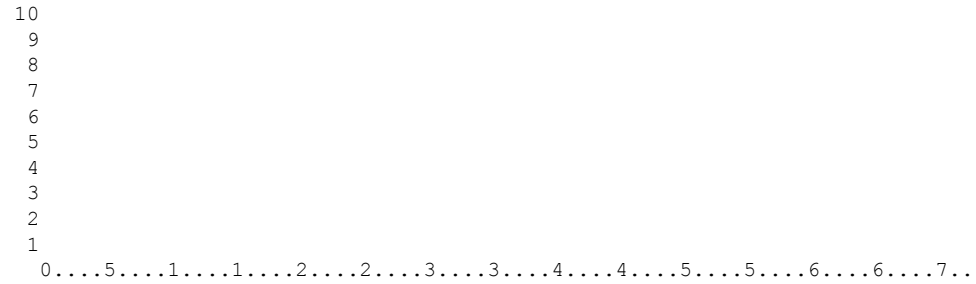


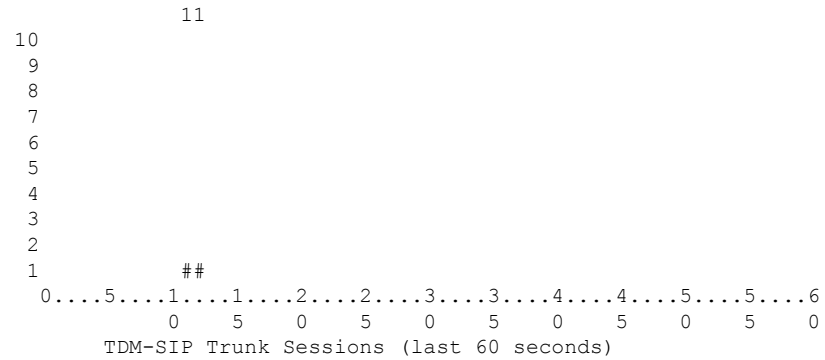
                                                    369863146641
                                                   8880900440044
                                                   3330922440011
 910                                                  **
 820                                                  #*
 730                                                  ##
 640                                                 *##*   **
 550                                                 ###*   ##
 460                                                 ####  *##*
 370                                                *####  *##*
 280                                                ######* ####
 190                                                ###### ####
 100                                               *######*####*
  10                                               ##############
    0....5....1....1....2....2....3....3....4....4....5....5....6
              0    5    0    5    0    5    0    5    0    5    0
         CUBE Standard Trunk License Usage (last 60 minutes)
         * = maximum     # = average



    9
    0
    0
 970
 890 *
 810 *
 730 *
 650 *
 570 *
 490 *
 410 *
 330 *
 250 *
 170 #
    0....5....1....1....2....2....3....3....4....4....5....5....6....6....7..
```

```
           0    5    0    5    0    5    0    5    0    5    0    5    0
      CUBE Standard Trunk License Usage (last 72 hours)
      * = maximum     # = average
```







```
   11
  10
   9
   8
   7
   6
   5
   4
   3
   2
   1 **
    0....5....1....1....2....2....3....3....4....4....5....5....6....6....7..
              0    5    0    5    0    5    0    5    0    5    0    5    0
         TDM-SIP Trunk Sessions (last 72 hours)
         * = maximum   # = average
```

```
  10
   9
   8
   7
   6
   5
   4
   3
   2
   1
    0....5....1....1....2....2....3....3....4....4....5....5....6....6....7..
              0    5    0    5    0    5    0    5    0    5    0    5    0
         TDM-SIP Trunk Sessions (last 72 days)
         * = maximum   # = average
```

The following are sample outputs for **show voice sip license stats table** command:

```
cube#show voice sip license stats table

        02:50:16 PM Wednesday Nov 13 2019 UTC


CUBE Standard Trunk License Usage  (last 60 seconds)
Period     Average       Max
----------------------------
 1-5           0          0
 6-10          0          0
11-15          0          0
16-20          0          0
21-25          0          0
26-30          0          0
31-35          0          0
36-40          0          0
41-45          0          0
46-50          0          0
51-55          0          0
56-60          0          0


CUBE Standard Trunk License Usage  (last 60 minutes)
Period     Average       Max
```

```
----------------------------
 1-5           0          0
 6-10          0          0
11-15          0          0
16-20          0          0
21-25          0          0
26-30          0          0
31-35          0          0
36-40          0          0
41-45          0          0
46-50        324        900
51-55        343        899
56-60        292        600


CUBE Standard Trunk License Usage  (last 72 hours)
Period     Average       Max
----------------------------
 1-5          35        900
 6-10          0          0
11-15          0          0
16-20          0          0
21-25          0          0
26-30          0          0
31-35          0          0
36-40          0          0
41-45          0          0
46-50          0          0
51-55          0          0
56-60          0          0
61-65          0          0
66-70          0          0
71-72          0          0


CUBE Standard Trunk License Usage  (last 72 days)
Period     Average       Max
----------------------------
 1-5           0          0
 6-10          0          0
11-15          0          0
16-20          0          0
21-25          0          0
26-30          0          0
31-35          0          0
36-40          0          0
41-45          0          0
46-50          0          0
51-55          0          0
56-60          0          0
61-65          0          0
66-70          0          0
71-72          0          0

TDM-SIP Trunk Sessions (last 60 seconds)
Period        Average        Max
----------------------------
 1-5           0          0
 6-10          0          0
11-15          0          0
16-20          0          0
21-25          0          0
26-30          0          0
31-35          0          0
```

```
36-40           0           0
41-45           0           0
46-50           0           0
51-55           0           0
56-60           0           0


TDM-SIP Trunk Sessions (last 60 minutes)
Period        Average        Max
-----------------------------
 1-5            0           2
 6-10           0           1
11-15           0           1
16-20           0           1
21-25           0           0
26-30           0           0
31-35           0           0
36-40           0           0
41-45           0           0
46-50           0           0
51-55           0           0
56-60           0           0

TDM-SIP Trunk Sessions (last 72 hours)
Period        Average         Max
-----------------------------
 1-5            0           0
 6-10           0           0
11-15           0           0
16-20           0           0
21-25           0           0
26-30           0           0
31-35           0           0
36-40           0           0
41-45           0           0
46-50           0           0
51-55           0           0
56-60           0           0
61-65           0           0
66-70           0           0
71-72           0           0

TDM-SIP Trunk Sessions (last 72 days)
Period        Average         Max
-----------------------------
 1-5            0           0
 6-10           0           0
11-15           0           0
16-20           0           0
21-25           0           0
26-30           0           0
31-35           0           0
36-40           0           0
41-45           0           0
46-50           0           0
51-55           0           0
56-60           0           0
61-65           0           0
66-70           0           0
71-72           0           0
```

The following example shows output of **show voice sip license status** command when SIP service is enabled:

```
cube#show voice sip license status

Host Name: cube
Current Time: Nov 25 2019 14:46:41 IST
SIP service: Up
License request interval: 5 Minute(s)
Next request at: Nov 25 2019 14:50:44 IST
Recent request(s) for CUBE Standard Trunk
-------------------------------------------------------------
Timestamp                   Count        Result
-------------------------------------------------------------
Nov 25 2019 14:45:44 IST    10           Out of compliance
Nov 25 2019 14:40:44 IST    4            Authorized
Nov 25 2019 14:35:44 IST    2            Authorized
```

After the entitlement request is sent and before receiving the response, the "Result" column in the output shows the same value as that of the previous and appends it with "(Response Pending)". For example, in the following output, the response is awaited for the entitlement request that is sent at "Dec 5 2019 16:17:46 IST". Hence, the "Result" column shows "Authorized(Response Pending)". If the entitlement request is sent for the first time, then the "Result" is shown as "Unknown(Response Pending)".

```
cube#show voice sip license status

Host Name: cube
Current Time: Dec 5 2019 16:18:22 IST
SIP service: Up
License request interval: 1 Minute(s)
Next request at: Dec 5 2019 16:18:46 IST
Recent request(s) for CUBE Standard Trunk
-----------------------------------------------------------------------
Timestamp                   Count        Result
-----------------------------------------------------------------------
Dec 5 2019 16:17:46 IST     2            Authorized(Response Pending)
Dec 5 2019 15:59:46 IST     0            Authorized
Dec 5 2019 15:58:46 IST     1            Authorized
```

After receiving the response, the output is updated accordingly. Considering the above example, the result for the entitlement request that is sent at "Dec 5 2019 16:17:46 IST" will be updated as "Authorized" as shown below.

```
cube#show voice sip license status

Host Name: cube
Current Time: Dec 5 2019 16:18:32 IST
SIP service: Up
License request interval: 1 Minute(s)
Next request at: Dec 5 2019 16:18:46 IST
Recent request(s) for CUBE Standard Trunk
-----------------------------------------------------------------------
Timestamp                   Count        Result
-----------------------------------------------------------------------
Dec 5 2019 16:17:46 IST     2            Authorized
Dec 5 2019 15:59:46 IST     0            Authorized
Dec 5 2019 15:58:46 IST     1            Authorized
```

The entitlement request is sent only when there is a change in the license request count. For example, in the following output, license request interval is 5 minutes and a request was sent for a count of 3 at Nov 21 2019 14:29:50 IST. There was no change in the license usage during the 5-minute interval and therefore a request is not sent at Nov 21 2019 14:34:50 IST. The license usage got changed in the next 5-minute interval and therefore a request was sent at Nov 21 2019 14:39:50 IST.

```
cube#show voice sip license status

Host Name: cube
Current Time: Nov 22 2019 04:02:53 IST
SIP service: Up
License request interval: 5 Minute(s)
Next request at: Nov 22 2019 04:04:50 IST
Recent request(s) for CUBE Standard Trunk
------------------------------------------------------------
Time                        Count        Result
------------------------------------------------------------
Nov 21 2019 14:39:50 IST    0            Authorized
Nov 21 2019 14:29:50 IST    3            Authorized
```

The following example shows output of the **show voice sip license status** command when the evaluation period has expired and the SIP service is blocked. Although the SIP service is blocked, information about previous requests sent (when the SIP service was up) is available in the output. In the following example, a licenses request was sent for a count of 15 at Nov 26 2019 04:59:53 IST when the SIP service was up. After that, the SIP service was blocked due to expiry of evaluation period.

```
cube#show voice sip license status

Host Name: cube
Current Time: Nov 26 2019 05:03:08 IST
SIP service: blocked due to eval expiry
License request interval: 5 Minute(s)
Next request at: Nov 26 2019 05:04:53 IST
Recent request(s) for CUBE Standard Trunk
------------------------------------------------------------
Timestamp                   Count        Result
------------------------------------------------------------
Nov 26 2019 04:59:53 IST    15           Eval period
```

License Usage for WebSocket-based Forking in CUBE

The following is a sample output for license usage in tabular and graphical format for Standard CUBE trunk calls:

```
Router#show voice sip license stats table
CUBE Standard Trunk License Usage  (last 60 seconds)
Period     Average       Max
----------------------------
 1-5           1          1
 6-10          0          0
11-15          0          0
16-20          0          0
21-25          0          0
26-30          0          0
31-35          0          0
36-40          0          0
41-45          0          0
46-50          0          0
51-55          0          0
56-60          0          0


CUBE Standard Trunk License Usage  (last 60 minutes)
Period     Average       Max
----------------------------
```

```
 1-5           0          0
 6-10          0          0
11-15          0          0
16-20          0          0
21-25          0          0
26-30          0          0
31-35          0          0
36-40          0          0
41-45          0          0
46-50          0          0
51-55          0          0
56-60          0          0


CUBE Standard Trunk License Usage  (last 72 hours)
Period     Average       Max
----------------------------
 1-5           0          0
 6-10          0          0
11-15          0          0
16-20          2         99
21-25          0         40
26-30          0          0
31-35          0          0
36-40          0          0
41-45          0         43
46-50          0          0
51-55          0          0
56-60          0          0
61-65          0          0
66-70          0          0
71-72          0          0


CUBE Standard Trunk License Usage  (last 72 days)
Period     Average       Max
----------------------------
 1-5           0         99
 6-10          0          0
11-15          0          0
16-20          0          0
21-25          0          0
26-30          0          0
31-35          0          0
36-40          0          0
41-45          0          0
46-50          0          0
51-55          0          0
56-60          0          0
61-65          0          0
66-70          0          0
71-72          0          0

Router#show voice sip license stats




      111111111111
   10
    9
    8
    7
    6
```

```
  5
  4
  3
  2
  1 ############
   0....5....1....1....2....2....3....3....4....4....5....5....6
             0    5    0    5    0    5    0    5    0    5    0
        CUBE Standard Trunk License Usage (last 60 seconds)
```

```
 10
  9
  8
  7
  6
  5
  4
  3
  2
  1
   0....5....1....1....2....2....3....3....4....4....5....5....6
             0    5    0    5    0    5    0    5    0    5    0
        CUBE Standard Trunk License Usage (last 60 minutes)
        * = maximum   # = average
```

```
                   9 99 4 2                 4
                   9 99 0 1                 3
 100               * **
  90               * **
  80               * **
  70               * **
  60               * **
  50               * **
  40               * ** *                   *
  30               * ** *                   *
  20               * ** * *                 *
  10               * *# * *                 *
    0....5....1....1....2....2....3....3....4....4....5....5....6....6....7..
             0    5    0    5    0    5    0    5    0    5    0    5    0
        CUBE Standard Trunk License Usage (last 72 hours)
        * = maximum   # = average
```

```
    9
    9
 100
  99 *
  98 *
  97 *
  96 *
  95 *
  94 *
  93 *
  92 *
```

```
   91 *
   90 *
     0....5....1....1....2....2....3....3....4....4....5....5....6....6....7..
               0    5    0    5    0    5    0    5    0    5    0    5    0
          CUBE Standard Trunk License Usage (last 72 days)
          * = maximum   # = average
```

The following is a sample output for license usage in tabular and graphical format for Enhanced CUBE calls:

```
Router#show voice sip license stats table
CUBE Enhanced Trunk License Usage  (last 60 seconds)
Period     Average       Max
----------------------------
 1-5           0          0
 6-10          0          0
11-15          0          0
16-20          0          0
21-25          0          0
26-30          0          0
31-35          0          0
36-40          0          0
41-45          0          0
46-50          0          0
51-55          0          0
56-60          0          0

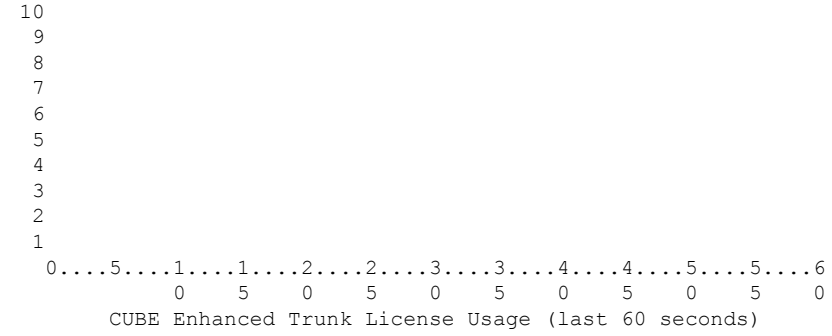

CUBE Enhanced Trunk License Usage  (last 60 minutes)
Period     Average       Max
----------------------------
 1-5           0          0
 6-10          0          0
11-15          0          0
16-20          0          0
21-25          0          0
26-30          0          0
31-35          0          0
36-40          0          0
41-45          0          0
46-50          0          0
51-55          0          0
56-60          0          0

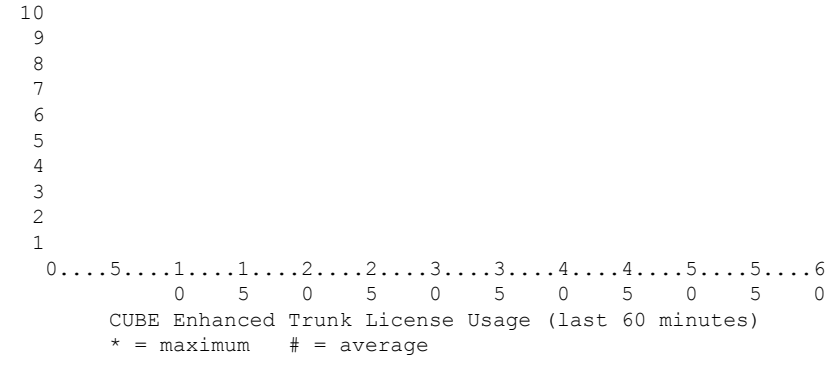

CUBE Enhanced Trunk License Usage  (last 72 hours)
Period     Average       Max
----------------------------
 1-5           0          0
 6-10          0          0
11-15          0          0
16-20          0         50
21-25          0         20
26-30          0          0
31-35          0          0
36-40          0          0
41-45          0         41
46-50          0          0
51-55          0          0
56-60          0          0
61-65          0          0
```

```
66-70           0           0
71-72           0           0

CUBE Enhanced Trunk License Usage  (last 72 days)
Period     Average       Max
---------------------------
 1-5            0          41
 6-10           0           0
11-15           0           0
16-20           0           0
21-25           0           0
26-30           0           0
31-35           0           0
36-40           0           0
41-45           0           0
46-50           0           0
51-55           0           0
56-60           0           0
61-65           0           0
66-70           0           0
71-72           0           0

Router#show voice sip license stats
```





```
                    5 53 221                  4
                    0 00 004                  1
 100
  90
  80
  70
  60
  50                * *
  40                * *                       *
  30                * **                      *
  20                * ** **                   *
  10                * ** ***                  *
    0....5....1....1....2....2....3....3....4....4....5....5....6....6....7..
              0    5    0    5    0    5    0    5    0    5    0    5    0
         CUBE Enhanced Trunk License Usage (last 72 hours)
         * = maximum   # = average
```

```
     4
     1
  50
  49
  48
  47
  46
  45
  44
  43
  42
  41 *
  40 *
    0....5....1....1....2....2....3....3....4....4....5....5....6....6....7..
              0    5    0    5    0    5    0    5    0    5    0    5    0
         CUBE Enhanced Trunk License Usage (last 72 days)
         * = maximum   # = average
```

The following is a sample output for license usage in tabular and graphical format for Aggregate trunk CUBE calls:

```
Router#show voice sip license stats table
CUBE Aggregate Trunk License Usage  (last 60 seconds)
Period     Average       Max
----------------------------
 1-5           0          0
 6-10          0          0
11-15          0          0
16-20          0          0
21-25          0          0
26-30          0          0
31-35          0          0
36-40          0          0
41-45          0          0
46-50          0          0
51-55          0          0
56-60          0          0


CUBE Aggregate Trunk License Usage  (last 60 minutes)
```

```
Period     Average       Max
----------------------------
 1-5           0          0
 6-10          0          0
11-15          0          0
16-20          0          0
21-25          0          0
26-30          0          0
31-35          0          0
36-40          0          0
41-45          0          0
46-50          0          0
51-55          0          0
56-60          0          0


CUBE Aggregate Trunk License Usage  (last 72 hours)
Period     Average       Max
----------------------------
 1-5           0          0
 6-10          0          0
11-15          0          0
16-20          0         50
21-25          0         20
26-30          0          0
31-35          0          0
36-40          0          0
41-45          0         41
46-50          0          0
51-55          0          0
56-60          0          0
61-65          0          0
66-70          0          0
71-72          0          0


CUBE Aggregate Trunk License Usage  (last 72 days)
Period     Average       Max
----------------------------
 1-5           0         41
 6-10          0          0
11-15          0          0
16-20          0          0
21-25          0          0
26-30          0          0
31-35          0          0
36-40          0          0
41-45          0          0
46-50          0          0
51-55          0          0
56-60          0          0
61-65          0          0
66-70          0          0
71-72          0          0

Router#show voice sip license stats



      11111111111111111
   10
```

```
 9
 8
 7
 6
 5
 4
 3
 2
 1 #################
  0....5....1....1....2....2....3....3....4....4....5....5....6
            0    5    0    5    0    5    0    5    0    5    0
       CUBE Aggregate Trunk License Usage (last 60 seconds)
```

```
 10
  9
  8
  7
  6
  5
  4
  3
  2
  1
   0....5....1....1....2....2....3....3....4....4....5....5....6
             0    5    0    5    0    5    0    5    0    5    0
       CUBE Aggregate Trunk License Usage (last 60 minutes)
       * = maximum   # = average
```

```
                  9 99 422                 8
                  9 99 001                 0
100               * **
 90               * **
 80               * **                     *
 70               * **                     *
 60               * **                     *
 50               * **                     *
 40               * ** *                   *
 30               * ** *                   *
 20               * ** ***                 *
 10               * *# ***                 *
   0....5....1....1....2....2....3....3....4....4....5....5....6....6....7..
             0    5    0    5    0    5    0    5    0    5    0    5    0
       CUBE Aggregate Trunk License Usage (last 72 hours)
       * = maximum   # = average
```

```
    9
    9
100
 99 *
 98 *
 97 *
 96 *
```

```
  95 *
  94 *
  93 *
  92 *
  91 *
  90 *
    0....5....1....1....2....2....3....3....4....4....5....5....6....6....7..
              0    5    0    5    0    5    0    5    0    5    0    5    0
         CUBE Aggregate Trunk License Usage (last 72 days)
         * = maximum   # = average
```

The license usage reporting for WebSockets in CUBE includes the summary of last 10 usage reports. The following is a sample output of **show voice sip license** for a CUBE router in B2BHA mode:

```
Router#show voice sip license status
Host Name: Router
Current Time: Apr 30 2021 07:37:12 UTC
SIP service: Up
License use recorded every: 7 Day(s)
Next record at: May 7 2021 07:00:00 UTC
Recent use of license(s) for CUBE Enhanced Trunk
--------------------------------------------------------------------------------
Timestamp                   Count
--------------------------------------------------------------------------------
Apr 30 2021 07:00:00 UTC    10
Apr 30 2021 05:55:11 UTC    1
Apr 30 2021 05:54:52 UTC    1
Router#sh log | sec LICENSE_INFO
*Apr 30 07:00:00.751: %CUBE-5-LICENSE_INFO: Requesting for 0 CUBE Enhanced trunk licenses
Router#sh voice sip license stats

Router   07:37:47 AM Friday Apr 30 2021 UTC
```

```
  10
   9
   8
   7
   6
   5
   4
   3
   2
   1
    0....5....1....1....2....2....3....3....4....4....5....5....6
              0    5    0    5    0    5    0    5    0    5    0
         CUBE Standard Trunk License Usage (last 60 seconds)
```

```
10
 9
 8
 7
 6
 5
 4
 3
 2
 1
  0....5....1....1....2....2....3....3....4....4....5....5....6
            0    5    0    5    0    5    0    5    0    5    0
       CUBE Standard Trunk License Usage (last 60 minutes)
       * = maximum   # = average
```

```
10
 9
 8
 7
 6
 5
 4
 3
 2
 1
  0....5....1....1....2....2....3....3....4....4....5....5....6....6....7..
            0    5    0    5    0    5    0    5    0    5    0    5    0
       CUBE Standard Trunk License Usage (last 72 hours)
       * = maximum   # = average
```

```
10
 9
 8
 7
 6
 5
 4
 3
 2
 1
  0....5....1....1....2....2....3....3....4....4....5....5....6....6....7..
            0    5    0    5    0    5    0    5    0    5    0    5    0
       CUBE Standard Trunk License Usage (last 72 days)
       * = maximum   # = average


Router   07:37:50 AM Friday Apr 30 2021 UTC
```

```
10
 9
 8
 7
 6
 5
 4
 3
 2
 1
  0....5....1....1....2....2....3....3....4....4....5....5....6
            0    5    0    5    0    5    0    5    0    5    0
       CUBE Enhanced Trunk License Usage (last 60 seconds)
```

```
10
 9
 8
 7
 6
 5
 4
 3
 2
 1
  0....5....1....1....2....2....3....3....4....4....5....5....6
            0    5    0    5    0    5    0    5    0    5    0
       CUBE Enhanced Trunk License Usage (last 60 minutes)
       * = maximum   # = average
```

```
   1
   0
20
19
18
17
16
15
14
13
12
11
10 *
  0....5....1....1....2....2....3....3....4....4....5....5....6....6....7..
            0    5    0    5    0    5    0    5    0    5    0    5    0
       CUBE Enhanced Trunk License Usage (last 72 hours)
       * = maximum   # = average
```

```
10
 9
 8
```

```
 7
 6
 5
 4
 3
 2
 1
  0....5....1....1....2....2....3....3....4....4....5....5....6....6....7..
            0    5    0    5    0    5    0    5    0    5    0    5    0
       CUBE Enhanced Trunk License Usage (last 72 days)
       * = maximum   # = average


Router   07:37:54 AM Friday Apr 30 2021 UTC




10
 9
 8
 7
 6
 5
 4
 3
 2
 1
  0....5....1....1....2....2....3....3....4....4....5....5....6
            0    5    0    5    0    5    0    5    0    5    0
       CUBE Aggregate Trunk License Usage (last 60 seconds)




10
 9
 8
 7
 6
 5
 4
 3
 2
 1
  0....5....1....1....2....2....3....3....4....4....5....5....6
            0    5    0    5    0    5    0    5    0    5    0
       CUBE Aggregate Trunk License Usage (last 60 minutes)
       * = maximum   # = average



   1
   0
  20
  19
  18
```

```
   17
   16
   15
   14
   13
   12
   11
   10 *
     0....5....1....1....2....2....3....3....4....4....5....5....6....6....7..
               0    5    0    5    0    5    0    5    0    5    0    5    0
          CUBE Aggregate Trunk License Usage (last 72 hours)
          * = maximum   # = average
```

```
   10
    9
    8
    7
    6
    5
    4
    3
    2
    1
     0....5....1....1....2....2....3....3....4....4....5....5....6....6....7..
               0    5    0    5    0    5    0    5    0    5    0    5    0
          CUBE Aggregate Trunk License Usage (last 72 days)
          * = maximum   # = average
```

```
Router   07:37:56 AM Friday Apr 30 2021 UTC
```

```
   10
    9
    8
    7
    6
    5
    4
    3
    2
    1
     0....5....1....1....2....2....3....3....4....4....5....5....6
               0    5    0    5    0    5    0    5    0    5    0
          TDM-SIP Trunk Sessions (last 60 seconds)
```

```
   10
    9
```

```
     8
     7
     6
     5
     4
     3
     2
     1
      0....5....1....1....2....2....3....3....4....4....5....5....6
                0    5    0    5    0    5    0    5    0    5    0
           TDM-SIP Trunk Sessions (last 60 minutes)
           * = maximum   # = average




    10
     9
     8
     7
     6
     5
     4
     3
     2
     1
      0....5....1....1....2....2....3....3....4....4....5....5....6....6....7..
                0    5    0    5    0    5    0    5    0    5    0    5    0
           TDM-SIP Trunk Sessions (last 72 hours)
           * = maximum   # = average



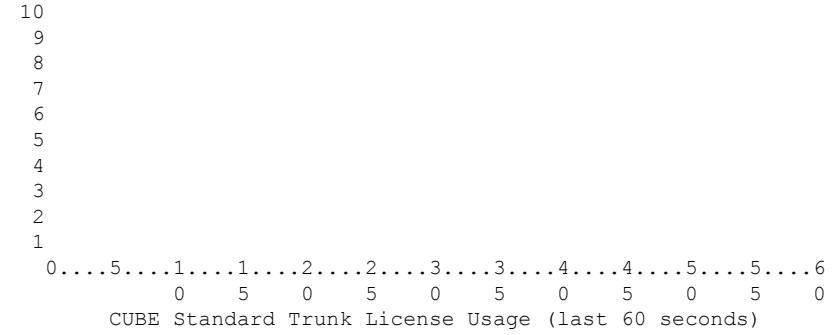

    10
     9
     8
     7
     6
     5
     4
     3
     2
     1
      0....5....1....1....2....2....3....3....4....4....5....5....6....6....7..
                0    5    0    5    0    5    0    5    0    5    0    5    0
           TDM-SIP Trunk Sessions (last 72 days)
           * = maximum   # = average
=============================================================================

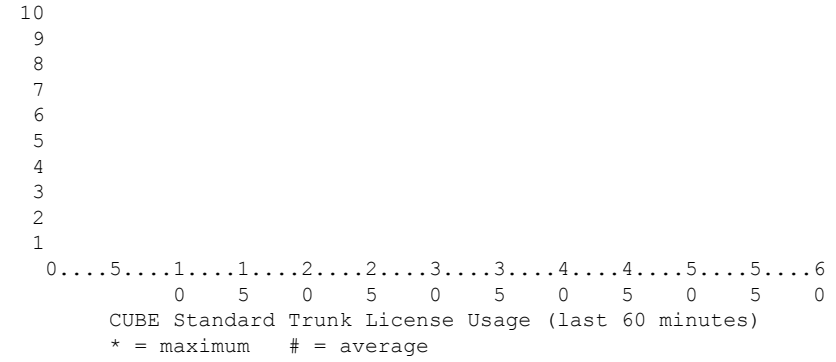
STANDBY:

Router#sh voice sip license status
Host Name: Router
Current Time: Apr 30 2021 07:37:26 UTC
SIP service: Up
License use recorded every: 7 Day(s)
Next record at: Timer not started
Recent use of license(s) for CUBE Enhanced Trunk
```

```
------------------------------------------------------------------------------
Timestamp                   Count
------------------------------------------------------------------------------
Apr 30 2021 05:55:11 UTC    1
Router#sh log | sec LICENSE_INFO
Router#
Router#
Router#sh voice sip license stats

Router   07:38:52 AM Friday Apr 30 2021 UTC
```







```
 2
 1
  0....5....1....1....2....2....3....3....4....4....5....5....6....6....7..
            0    5    0    5    0    5    0    5    0    5    0    5    0
       CUBE Standard Trunk License Usage (last 72 hours)
       * = maximum   # = average
```

```
10
 9
 8
 7
 6
 5
 4
 3
 2
 1
  0....5....1....1....2....2....3....3....4....4....5....5....6....6....7..
            0    5    0    5    0    5    0    5    0    5    0    5    0
       CUBE Standard Trunk License Usage (last 72 days)
       * = maximum   # = average
```

```
Router   07:38:52 AM Friday Apr 30 2021 UTC
```

```
10
 9
 8
 7
 6
 5
 4
 3
 2
 1
  0....5....1....1....2....2....3....3....4....4....5....5....6
            0    5    0    5    0    5    0    5    0    5    0
       CUBE Enhanced Trunk License Usage (last 60 seconds)
```

```
10
 9
 8
 7
 6
 5
 4
 3
```

```
 2
 1
  0....5....1....1....2....2....3....3....4....4....5....5....6
            0    5    0    5    0    5    0    5    0    5    0
       CUBE Enhanced Trunk License Usage (last 60 minutes)
       * = maximum   # = average




    1
    0
   20
   19
   18
   17
   16
   15
   14
   13
   12
   11
   10 *
    0....5....1....1....2....2....3....3....4....4....5....5....6....6....7..
            0    5    0    5    0    5    0    5    0    5    0    5    0
       CUBE Enhanced Trunk License Usage (last 72 hours)
       * = maximum   # = average\




   10
    9
    8
    7
    6
    5
    4
    3
    2
    1
    0....5....1....1....2....2....3....3....4....4....5....5....6....6....7..
            0    5    0    5    0    5    0    5    0    5    0    5    0
       CUBE Enhanced Trunk License Usage (last 72 days)
       * = maximum   # = average


Router   07:38:57 AM Friday Apr 30 2021 UTC




   10
    9
    8
    7
    6
    5
    4
```

```
 3
 2
 1
  0....5....1....1....2....2....3....3....4....4....5....5....6
            0    5    0    5    0    5    0    5    0    5    0
       CUBE Aggregate Trunk License Usage (last 60 seconds)
```

```
10
 9
 8
 7
 6
 5
 4
 3
 2
 1
  0....5....1....1....2....2....3....3....4....4....5....5....6
            0    5    0    5    0    5    0    5    0    5    0
       CUBE Aggregate Trunk License Usage (last 60 minutes)
       * = maximum   # = average
```

```
   1
   0
20
19
18
17
16
15
14
13
12
11
10 *
  0....5....1....1....2....2....3....3....4....4....5....5....6....6....7..
            0    5    0    5    0    5    0    5    0    5    0    5    0
       CUBE Aggregate Trunk License Usage (last 72 hours)
       * = maximum   # = average
```

```
10
 9
 8
 7
 6
 5
 4
 3
 2
 1
```

```
 0....5....1....1....2....2....3....3....4....4....5....5....6....6....7..
           0    5    0    5    0    5    0    5    0    5    0    5    0
      CUBE Aggregate Trunk License Usage (last 72 days)
      * = maximum   # = average


Router   07:38:58 AM Friday Apr 30 2021 UTC




  10
   9
   8
   7
   6
   5
   4
   3
   2
   1
    0....5....1....1....2....2....3....3....4....4....5....5....6
              0    5    0    5    0    5    0    5    0    5    0
         TDM-SIP Trunk Sessions (last 60 seconds)




  10
   9
   8
   7
   6
   5
   4
   3
   2
   1
    0....5....1....1....2....2....3....3....4....4....5....5....6
              0    5    0    5    0    5    0    5    0    5    0
         TDM-SIP Trunk Sessions (last 60 minutes)
         * = maximum   # = average




  10
   9
   8
   7
   6
   5
   4
   3
   2
   1
```

```
 0....5....1....1....2....2....3....3....4....4....5....5....6....6....7..
           0    5    0    5    0    5    0    5    0    5    0    5    0
      TDM-SIP Trunk Sessions (last 72 hours)
      * = maximum   # = average




10
 9
 8
 7
 6
 5
 4
 3
 2
 1
 0....5....1....1....2....2....3....3....4....4....5....5....6....6....7..
           0    5    0    5    0    5    0    5    0    5    0    5    0
      TDM-SIP Trunk Sessions (last 72 days)
      * = maximum   # = average
```

The license usage reporting for WebSockets in CUBE includes the summary of last 10 usage reports. The following is a sample output of **show voice sip license** for a CUBE router in Standalone mode:

```
Router#show voice sip license status
Host Name: Router
Current Time: Mar 30 2021 00:32:35 UTC
SIP service: Up
License use recorded every: 8 Hour(s)
Next record at: Mar 30 2021 07:00:00 UTC
Recent use of license(s) for CUBE Standard Trunk
--------------------------------------------------------------------------------
Timestamp                   Count
--------------------------------------------------------------------------------
Mar 29 2021 23:00:00 UTC    0
Mar 29 2021 22:00:00 UTC    9
Mar 29 2021 21:00:00 UTC    24
Mar 29 2021 20:00:00 UTC    13
Mar 29 2021 11:00:00 UTC    0
Mar 29 2021 09:00:00 UTC    2
Recent use of license(s) for CUBE Enhanced Trunk
--------------------------------------------------------------------------------
Timestamp                   Count
--------------------------------------------------------------------------------
Mar 29 2021 21:00:00 UTC    0
Mar 29 2021 20:00:00 UTC    2
Mar 29 2021 11:00:00 UTC    0
Mar 29 2021 09:00:00 UTC    8

========================================

Router#sh voice sip license stats

Router   12:34:22 AM Tuesday Mar 30 2021 UTC
```

```
 10
  9
  8
  7
  6
  5
  4
  3
  2
  1
   0....5....1....1....2....2....3....3....4....4....5....5....6
             0    5    0    5    0    5    0    5    0    5    0
       CUBE Standard Trunk License Usage (last 60 seconds)
```

```
 10
  9
  8
  7
  6
  5
  4
  3
  2
  1
   0....5....1....1....2....2....3....3....4....4....5....5....6
             0    5    0    5    0    5    0    5    0    5    0
       CUBE Standard Trunk License Usage (last 60 minutes)
       * = maximum   # = average
```

```
       21         1
      943         0
100
 90
 80
 70
 60
 50
 40
 30
 20     *
 10    ***         *
   0....5....1....1....2....2....3....3....4....4....5....5....6....6....7..
             0    5    0    5    0    5    0    5    0    5    0    5    0
       CUBE Standard Trunk License Usage (last 72 hours)
       * = maximum   # = average
```

```
 10
  9
  8
```

```
 7
 6
 5
 4
 3
 2
 1
  0....5....1....1....2....2....3....3....4....4....5....5....6....6....7..
            0    5    0    5    0    5    0    5    0    5    0    5    0
       CUBE Standard Trunk License Usage (last 72 days)
       * = maximum   # = average


Router   12:34:23 AM Tuesday Mar 30 2021 UTC




10
 9
 8
 7
 6
 5
 4
 3
 2
 1
  0....5....1....1....2....2....3....3....4....4....5....5....6
            0    5    0    5    0    5    0    5    0    5    0
       CUBE Enhanced Trunk License Usage (last 60 seconds)




10
 9
 8
 7
 6
 5
 4
 3
 2
 1
  0....5....1....1....2....2....3....3....4....4....5....5....6
            0    5    0    5    0    5    0    5    0    5    0
       CUBE Enhanced Trunk License Usage (last 60 minutes)
       * = maximum   # = average



        2         8
10
 9
 8               *
```

```
 7                *
 6                *
 5                *
 4                *
 3                *
 2      *         *
 1      *         *
  0....5....1....1....2....2....3....3....4....4....5....5....6....6....7..
            0    5    0    5    0    5    0    5    0    5    0    5    0
       CUBE Enhanced Trunk License Usage (last 72 hours)
       * = maximum   # = average
```

```
10
 9
 8
 7
 6
 5
 4
 3
 2
 1
  0....5....1....1....2....2....3....3....4....4....5....5....6....6....7..
            0    5    0    5    0    5    0    5    0    5    0    5    0
       CUBE Enhanced Trunk License Usage (last 72 days)
       * = maximum   # = average
```

```
Router   12:34:25 AM Tuesday Mar 30 2021 UTC
```

```
10
 9
 8
 7
 6
 5
 4
 3
 2
 1
  0....5....1....1....2....2....3....3....4....4....5....5....6
            0    5    0    5    0    5    0    5    0    5    0
       CUBE Aggregate Trunk License Usage (last 60 seconds)
```

```
10
 9
 8
```

```
  7
  6
  5
  4
  3
  2
  1
   0....5....1....1....2....2....3....3....4....4....5....5....6
             0    5    0    5    0    5    0    5    0    5    0
        CUBE Aggregate Trunk License Usage (last 60 minutes)
        * = maximum   # = average\




        21         1
       945         0
 100
  90
  80
  70
  60
  50
  40
  30
  20     **
  10    ***         *
    0....5....1....1....2....2....3....3....4....4....5....5....6....6....7..
             0    5    0    5    0    5    0    5    0    5    0    5    0
        CUBE Aggregate Trunk License Usage (last 72 hours)
        * = maximum   # = average




  10
   9
   8
   7
   6
   5
   4
   3
   2
   1
    0....5....1....1....2....2....3....3....4....4....5....5....6....6....7..
             0    5    0    5    0    5    0    5    0    5    0    5    0
        CUBE Aggregate Trunk License Usage (last 72 days)
        * = maximum   # = average


Router   12:34:25 AM Tuesday Mar 30 2021 UTC




  10
   9
   8
```

```
 7
 6
 5
 4
 3
 2
 1
  0....5....1....1....2....2....3....3....4....4....5....5....6
            0    5    0    5    0    5    0    5    0    5    0
       TDM-SIP Trunk Sessions (last 60 seconds)
```

```
10
 9
 8
 7
 6
 5
 4
 3
 2
 1
  0....5....1....1....2....2....3....3....4....4....5....5....6
            0    5    0    5    0    5    0    5    0    5    0
       TDM-SIP Trunk Sessions (last 60 minutes)
       * = maximum   # = average
```

```
10
 9
 8
 7
 6
 5
 4
 3
 2
 1
  0....5....1....1....2....2....3....3....4....4....5....5....6....6....7..
            0    5    0    5    0    5    0    5    0    5    0    5    0
       TDM-SIP Trunk Sessions (last 72 hours)
       * = maximum   # = average
```

```
10
 9
 8
 7
 6
 5
 4
```

```
3
2
1
 0....5....1....1....2....2....3....3....4....4....5....5....6....6....7..
           0    5    0    5    0    5    0    5    0    5    0    5    0
      TDM-SIP Trunk Sessions (last 72 days)
      * = maximum   # = average
```

show voice source-group

To display the details of one or more voice source IP groups, use the **show voice source-group** command in privileged EXEC mode.

show voice source-group [*name* | **sort** [**ascending** | **descending**]]

Syntax Description

name	(Optional) Name of the source IP group to display.
sort [**ascending** | **descending**	(Optional) Displays the source IP groups in either ascending or descending alphanumerical order.

Command Default

Ascending order

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.2(11)T	This command was introduced.

Examples

The following sample output shows an invalid configuration.

```
Router# show voice source-group abc
Source Group: abc
    description="",
    carrier-id source="sj_area",
    carrier-id target="",
    trunk-group-label source="",
    trunk-group-label target="ny_main",
    h323zone-id="",
    access-list=,
    disconnect-cause="no-service",
    translation-profile="",
```

The following sample output shows a valid configuration for carrier-ID routing:

```
Router# show voice source-group abc
Source Group: abc
    description="",
    carrier-id source="",
    carrier-id target="",
    trunk-group-label source="texas_backup",
    trunk-group-label target="ny_main",
    h323zone-id="",
    access-list=,
    disconnect-cause="no-service",
    translation-profile="",
```

If you are using carrier-ID routing, both carrier-ID fields are filled in and the "trunk-group-label" fields are blank.

The following sample output displays the source groups in ascending order. Both source IP groups use carrier-ID routing.

```
Router# show voice source-group sort ascending
Source Group:1
        description="routec calls from 1311 to 1411",
        carrier-id source="1311",
        carrier-id target="1411",
        trunk-group-label source="",
        trunk-group-label target="",
        h323zone-id="fr1311",
        access-list= ,
        disconnect-cause="user-busy",
        destination-pattern="",
        incoming called-number="",
        translation-profile="10",
Source Group:2
        description="",
        carrier-id source="abcd",
        carrier-id target="xyz",
        trunk-group-label source="",
        trunk-group-label target="",
        h323zone-id="",
        access-list= ,
        disconnect-cause="no-service",
        destination-pattern="",
        incoming called-number="",
        translation-profile="",
```

The table below describes significant fields shown in this output.

Table 191: show voice source-group Field Descriptions

Field	Description
Source Group	Name of the voice source IP group.
description	Description of the voice source IP group.
carrier-id source	Name of the source carrier ID used by the terminating gateway to select a target carrier.
carrier-id target	Name of the target carrier ID used by the terminating gateway to select a dial peer for routing the call over a POTS line.
trunk-group-label source	Name of the source trunk group used by the originating gateway to route the call over an inbound dial peer.
trunk-group-label target	Name of the target trunk group used by the terminating gateway to select a dial peer for routing an outbound call over a POTS line.
h323zone-id	Name of the zone associated with incoming H.323 calls to the voice source IP group.
access-list	Number of the access list used by the voice source IP group to block calls.
disconnect-cause	Phrase returned by the voice source IP group when a call is blocked.

Field	Description
translation-profile	Name of the translation profile used by the voice source IP group to translate calls.

Related Commands

Command	Description
voice source-group	Initiates a voice source IP group definition.

show voice statistics csr interval accounting

To display accounting statistics by configured intervals, use the **show voice statistics** csr interval **accounting**command in privileged EXEC mode.

show voice statistics csr interval *tag-number* **accounting** {**all** | **method-list** *method-list-name*} [**push** {**all** | **ftp** | **syslog**}]

Syntax Description

tag-number	Interval that represents a specified time range. The valid range is from 1 to 36655. **Note** You must first enter the **show voice statistics interval-tag** command to obtain the valid tag numbers that you can enter for this command.
all	Displays all voice accounting statistics.
method-list-name *method-list-name*	Displays accounting statistics by method list. You must specify a method-list name.
push	(Optional) Statistics are downloaded to an FTP or syslog server, or to both servers. The keywords are as follows: • all--Pushes statistics to both the FTP and syslog servers. • ftp--Pushes statistics to the FTP server. • syslog--Pushes statistics to the syslog server.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.3(4)T	This command was introduced.

Examples

The following sample output shows all of the statistics that were collected for interval tag 102 for method list h323-1:

```
Router# show voice statistics csr interval 102 accounting method-list h323-1
Client Type: Voice ACCT Stats
        Start Time: 2002-05-01T19:35:17Z        End Time: 2002-05-01T19:36:29Z
methodlist=h323-1,acc_pass_criteria=1,pstn_in_pass=0,pstn_in_fail=0,pstn_out_pass=0,
pstn_out_fail=0,ip_in_pass=0,ip_in_fail=0,ip_out_pass=0,ip_out_fail=0
```

The table below lists and describes the significant output fields.

Table 192: show voice statistics csr interval accounting Field Descriptions

Field	Description
Client Type	The type of statistics collected.

Field	Description
Start Time	The start time of the statistics collection.
End Time	The ending time of the statistics collection.
method-list	The method list name.
acc_pass_criteria	Accounting pass criteria: • 1: all start/interim/stop messages passed. • 2: all start/stop messages passed. • 3: stop-only message passed.
pstn_in_pass	Number of incoming calls on the PSTN leg that meet acc_pass_criteria.
pstn_in_fail	Number of incoming calls on the PSTN leg that fail acc_pass_criteria.
pstn_out_pass	Number of outgoing calls on the PSTN leg that meet acc_pass_criteria.
pstn_out_fail	Number of outgoing calls on the PSTN leg that fail acc_pass_criteria.
ip_in_pass	Number of incoming calls on the IP leg that meet acc_pass_criteria.
ip_in_fail	Number of incoming calls on the IP leg that fail acc_pass_criteria.
ip_out_pass	Number of outgoing calls on the IP leg that meet acc_pass_criteria.
ip_out_fail	Number of outgoing calls on the IP leg that fail acc_pass_criteria.

Related Commands

Command	Description
show event-manager consumers	Displays event-manager statistics.
show voice statistics csr interval aggregation	Displays statistical information by configured intervals for signaling statistics.
show voice statistics csr since-reset accounting	Displays all accounting CSRs since the last reset.
show voice statistics csr since-reset aggregation-level	Displays all signaling CSRs since the last reset.
show voice statistics csr since-reset all	Displays all CSRs since the last reset.
show voice statistics interval-tag	Displays the configured interval numbers.
show voice statistics memory-usage	Displays current memory usage.

show voice statistics csr interval aggregation

To display signaling statistics by configured intervals, use the **show voice statistics** csr interval aggregation command in privileged EXEC mode.

show voice statistics csr interval *tag-number* **aggregation** {**all** | **gateway** | **ip** | **pstn** | **trunk-group** {*trunk-group-labe* **l** | **all**} | **voice-port** {*voice-port-label* | **all**}} [**mode** {**concise** | **verbose**}] [**push** {**all** | **ftp** | **syslog**}]

Syntax Description

tag-number	Interval that represents a specified time range. The valid range is from 1 to 36655. **Note** You must first enter the **show voice statistics interval-tag**command to obtain the valid tag numbers that you can enter for this command.
all	Displays all levels of signaling statistics.
gateway	Displays gateway-wide level statistics.
ip	Displays VoIP interface level statistics.
pstn	Displays telephone interface level statistics.
trunk-group	Displays trunk-group level statistics. • *trunk-group-label* --displays statistics for a specific trunk group • **all** --Displays statistics for all trunk groups.
voice-port	Displays voice-port level statistics: • *voice-port-label* --displays statistics for a specific voice port • **all** --Displays statistics for all voice ports.
mode	(Optional) Statistics are displayed in a specified mode. The keywords are as follows: • concise--Displays output that contains total calls, answered calls, and answered call duration. • verbose--Displays all fields contained in call statistic records (CSRs). This is the default setting.
push	(Optional) Statistics are downloaded to an FTP or syslog server, or to both servers. The keywords are as follows: • all--Pushes statistics to both the FTP and syslog servers. • ftp--Pushes statistics to the FTP server. • syslog--Pushes statistics to the syslog server.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.3(4)T	This command was introduced.

Usage Guidelines

This command is valid only if the **voice statistics time-range** command is configured to either the **periodic** or **start-stop** value. If you enter the **show voice statistics csr interval aggregation**command but the gateway has been configured to collect statistics only since the last reset, the gateway displays an error message.

You must first enter the **show voice statistics interval-tag** to obtain the valid tag numbers that you can enter for this command.

Examples

The following sample output shows signaling statistics for all aggregation levels for interval tag 200:

```
Router# show voice statistics csr interval 200 aggregation all
Client Type: VCSR
        Start Time: 2002-04-28T01:48:24Z        End Time: 2002-04-28T01:50:01Z
record_type=gw,trunk_group_id=,voice_port_id=,in_call=0,in_ans=0,in_fail=0,out_call=0,
out_ans=0,out_fail=0,in_szre_d=0,out_szre_d=0,in_conn_d=0,out_conn_d=0,orig_disconn=0,
in_ans_abnorm=0,out_ans_abnorm=0,in_mcd=0,out_mcd=0,in_pdd=0,out_pdd=0,in_setup_delay=0,
out_setup_delay=0,lost_pkt=0,latency=0,jitter=0,in_disc_cc_16=0,out_disc_cc_16=0
!
record_type=ip,trunk_group_id=,voice_port_id=,in_call=0,in_ans=0,in_fail=0,out_call=0,
out_ans=0,out_fail=0,in_szre_d=0,out_szre_d=0,in_conn_d=0,out_conn_d=0,orig_disconn=0,
in_ans_abnorm=0,out_ans_abnorm=0,in_mcd=0,out_mcd=0,in_pdd=0,out_pdd=0,in_setup_delay=0,
out_setup_delay=0,lost_pkt=0,latency=0,jitter=0,in_disc_cc_16=0,out_disc_cc_16=0
!
record_type=pstn,trunk_group_id=,voice_port_id=,in_call=0,in_ans=0,in_fail=0,out_call=0,
out_ans=0,out_fail=0,in_szre_d=0,out_szre_d=0,in_conn_d=0,out_conn_d=0,orig_disconn=0,
in_ans_abnorm=0,out_ans_abnorm=0,in_mcd=0,out_mcd=0,in_pdd=0,out_pdd=0,in_setup_delay=0,
out_setup_delay=0,in_disc_cc_16=0,out_disc_cc_16=0
!
record_type=vp,trunk_group_id=,voice_port_id=4/0/0,in_call=0,in_ans=0,in_fail=0,
out_call=0,out_ans=0,out_fail=0,in_szre_d=0,out_szre_d=0,in_conn_d=0,out_conn_d=0,
orig_disconn=0,in_ans_abnorm=0,out_ans_abnorm=0,in_mcd=0,out_mcd=0,in_pdd=0,out_pdd=0,
in_setup_delay=0,out_setup_delay=0,in_disc_cc_16=0,out_disc_cc_16=0
!
record_type=vp,trunk_group_id=,voice_port_id=4/0/1,in_call=0,in_ans=0,in_fail=0,
out_call=0,out_ans=0,out_fail=0,in_szre_d=0,out_szre_d=0,in_conn_d=0,out_conn_d=0,
orig_disconn=0,in_ans_abnorm=0,out_ans_abnorm=0,in_mcd=0,out_mcd=0,in_pdd=0,out_pdd=0,
in_setup_delay=0,out_setup_delay=0,in_disc_cc_16=0,out_disc_cc_16=0
!
record_type=vp,trunk_group_id=,voice_port_id=4/1/0,in_call=0,in_ans=0,in_fail=0,
out_call=0,out_ans=0,out_fail=0,in_szre_d=0,out_szre_d=0,in_conn_d=0,out_conn_d=0,
orig_disconn=0,in_ans_abnorm=0,out_ans_abnorm=0,in_mcd=0,out_mcd=0,in_pdd=0,out_pdd=0,
in_setup_delay=0,out_setup_delay=0,in_disc_cc_16=0,out_disc_cc_16=0
!
record_type=vp,trunk_group_id=,voice_port_id=4/1/1,in_call=0,in_ans=0,in_fail=0,
out_call=0,out_ans=0,out_fail=0,in_szre_d=0,out_szre_d=0,in_conn_d=0,out_conn_d=0,
orig_disconn=0,in_ans_abnorm=0,out_ans_abnorm=0,in_mcd=0,out_mcd=0,in_pdd=0,out_pdd=0,
in_setup_delay=0,out_setup_delay=0,in_disc_cc_16=0,out_disc_cc_16=0
!
record_type=vp,trunk_group_id=,voice_port_id=2/0:23,in_call=0,in_ans=0,in_fail=0
,out_call=0,out_ans=0,out_fail=0,in_szre_d=0,out_szre_d=0,in_conn_d=0,out_conn_d=0,
orig_disconn=0,in_ans_abnorm=0,out_ans_abnorm=0,in_mcd=0,out_mcd=0,in_pdd=0,out_pdd=0,
in_setup_delay=0,out_setup_delay=0,in_disc_cc_16=0,out_disc_cc_16=0
!
```

```
record_type=vp,trunk_group_id=,voice_port_id=2/1:23,in_call=0,in_ans=0,in_fail=0
out_call=0,out_ans=0,out_fail=0,in_szre_d=0,out_szre_d=0,in_conn_d=0,out_conn_d=0,
orig_disconn=0,in_ans_abnorm=0,out_ans_abnorm=0,in_mcd=0,out_mcd=0,in_pdd=0,out_pdd=0,
in_setup_delay=0,out_setup_delay=0,in_disc_cc_16=0,out_disc_cc_16=0
```

The table below lists and describes the significant output fields.

Table 193: show voice statistics csr interval aggregation Field Descriptions

Field	Description
Client Type	The type of statistics collected.
Start Time	The start time of the statistics collection.
End Time	The ending time of the statistics collection.
record_type	Call statistics record type. Symbols are gw, ip, pstn, tg, and vp.
trunk_group_id	Trunk group ID. **Note** For the symbols gw, ip, pstn, and some vp records, this field is empty.
voice_port_id	Voice port ID. **Note** For the symbols gw, ip, pstn, and some vp records, this field is empty.
in_call	Number of incoming calls.
in_ans	Number of incoming calls answered by the gateway.
in_fail	Number of incoming calls that failed.
out_call	Number of outgoing calls attempted.
out_ans	Number of outgoing calls that received answers.
out_fail	Number of outgoing calls that failed.
in_szre_d	Incoming seizure duration (in seconds).
out_szre_d	Outgoing seizure duration (in seconds).
in_conn_d	Incoming connected duration (in seconds).
out_conn_d	Outgoing connected duration (in seconds).
orig_disconn	Number of calls encountering the originating side having been disconnected before the outgoing calls were connected.
in_ans_abnorm	Number of incoming answered calls terminated with any cause code other than "normal".
out_ans_abnorm	Number of outgoing answered calls terminated with any cause code other than "normal".
in_mcd	Number of incoming calls lasting less than the configured minimum call duration (MCD).

Field	Description
out_mcd	Number of outgoing calls lasting less than the configured MCD.
in_pdd	Total post dial delay duration on incoming calls (in ms).
out_pdd	Total post dial delay duration on outgoing calls (in ms).
in_setup_delay	Total inbound setup delay duration (in ms).
out_setup_delay	Total outbound setup delay duration (in ms).
lost_pkt	Number of calls losing more than the configured number of packets. **Note** This field will exist only in IP records. In other types of records, this field will be empty and extra commas are expected.
latency	Number of calls encountering more than the configured amount of latency. **Note** This field will exist only in IP records. In other types of records, this field will be empty and extra commas are expected.
jitter	Number of calls encountering more than configured amount of jitter. **Note** This field will exist only in IP records. In other types of records, this field will be empty and extra commas are expected.
in_cc_no	Number of the following disconnect cause code counters as per incoming calls (expected to be fewer than 5).
in_disc_cc	Incoming disconnect cause code. For example, in_disc_cc_16=3 indicates that 3 calls were disconnected or finished with a disconnect cause code of 16 (normal).
out_disc_cc	Outgoing disconnect cause code.
out_cc_no	Number of the following disconnect cause code counters as per outgoing calls (expected to be fewer than 5).
in_cc_id	Disconnect cause code ID for the following field for incoming calls.
in_cc_cntr	Disconnect cause code counter for incoming calls (any incoming cause code counter pairs).
out_cc_id	Disconnect cause code ID for the following field for outgoing calls.
out_cc_cntr	Disconnect cause code counter for outgoing calls (any outgoing cause code counter pairs).

Related Commands

Command	Description
show event-manager consumers	Displays event statistics.

Command	Description
show voice statistics csr interval accounting	Displays statistical information by configured intervals for accounting statistics.
show voice statistics csr since-reset accounting	Displays all accounting CSRs since the last reset.
show voice statistics csr since-reset aggregation-level	Displays all signaling CSRs since the last reset.
show voice statistics csr since-reset all	Displays all CSRs since the last reset.
show voice statistics interval-tag	Displays the configured interval numbers.
show voice statistics memory-usage	Displays current memory usage.
voice statistics time-range	Specifies the time range to collect CSRs.

show voice statistics csr since-reset accounting

To display VoIP AAA accounting statistics since the last reset, use the **show voice statistics** csr since-reset accounting command in privileged EXEC mode.

show voice statistics csr since-reset accounting {**all** | **method-list** *method-list-name*} [**push** {**all** | **ftp** | **syslog**}]

Syntax Description

all	All collected statistics since the last reset are displayed.
method-list *method-list-name*	Collected statistics by method list since the last reset are displayed. The method-list-name argument specifies the name of the method list.
push	(Optional) Statistics are downloaded to an FTP or syslog server, or to both servers. The keywords are as follows: • all--Pushes statistics to both the FTP and syslog servers. • ftp--Pushes statistics to the FTP server. • syslog--Pushes statistics to the syslog server.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.3(4)T	This command was introduced.

Usage Guidelines

This command only applies if the **voice statistics time-range** command is configured to the **since-reset**value. Voice statistics collection on the gateway is reset using the **clear voice statistics csr**command.

If you enter the **show voice statistics csr since-reset accounting**command but the gateway has been configured for periodic collection or to a specific interval, the gateway will display an error message.

Examples

The following sample output shows the accounting statistics for method list h323-1 since the last reset:

```
Router# show voice statistics csr since-reset accounting method-list h323-1
Client Type: Voice ACCT Stats
        Start Time: 2002-05-05T17:39:17Z        End Time: 2002-05-09T19:00:16Z
methodlist=h323-1,acc_pass_criteria=1,pstn_in_pass=0,pstn_in_fail=1,pstn_out_pass=0,
pstn_out_fail=0,ip_in_pass=0,ip_in_fail=0,ip_out_pass=0,ip_out_fail=1
```

The table below lists and describes the significant output fields.

Table 194: show voice statistics csr since-reset accounting Field Descriptions

Field	Description
Client Type	The type of statistics collected.

Field	Description
Start Time	The start time of the statistics collection.
End Time	The ending time of the statistics collection.
method-list	The method list name.
acc_pass_criteria	Accounting pass criteria: • 1: all start/interim/stop messages passed. • 2: all start/stop messages passed. • 3: stop-only message passed.
pstn_in_pass	Number of incoming calls on the PSTN leg that meet acc_pass_criteria.
pstn_in_fail	Number of incoming calls on the PSTN leg that fail acc_pass_criteria.
pstn_out_pass	Number of outgoing calls on the PSTN leg that meet acc_pass_criteria.
pstn_out_fail	Number of outgoing calls on the PSTN leg that fail acc_pass_criteria.
ip_in_pass	Number of incoming calls on the IP leg that meet acc_pass_criteria.
ip_in_fail	Number of incoming calls on the IP leg that fail acc_pass_criteria.
ip_out_pass	Number of outgoing calls on the IP leg that meet acc_pass_criteria.
ip_out_fail	Number of outgoing calls on the IP leg that fail acc_pass_criteria.

Related Commands

Command	Description
clear voice statistics	Clears voice statistics, resetting the statistics collection.
show event-manager consumers	Displays event statistics.
show voice statistics csr interval accounting	Displays statistical information by configured intervals for accounting statistics.
show voice statistics csr interval aggregation	Displays statistical information by configured intervals for signaling statistics.
show voice statistics csr since-reset aggregation-level	Displays all signaling CSRs since the last reset.
show voice statistics interval-tag	Displays the configured interval numbers
show voice statistics memory-usage	Displays current memory usage.
voice statistics time-range	Specifies a time range to collect statistics from the gateway on a periodic basis, since the last reset, or for a specific time duration.

show voice statistics csr since-reset aggregation-level

To display signaling statistics since the last reset, use the **show voice statistics** csr since-reset aggregation-level command in privileged EXEC mode.

show voice statistics csr since-reset aggregation-level {**all** | **gateway** | **ip** | **pstn** | **trunk-group** {**all***trunk-group-label*} | **voice-port** {**all***voice-port-label*}} [**mode** {**concise** | **verbose**}] [**push** {**all** | **ftp** | **syslog**}]

Syntax Description

all	All signaling statistics.
gateway	Gateway-wide level statistics.
ip	VoIP-interface-level statistics.
pstn	PSTN-level statistics.
trunk-group	Trunk-group-level statistics. Keywords and arguments are as follows. • **all** --Statistics for all trunk groups. • *trunk-group-label* --Statistics for a specific trunk group.
voice-port	Voice-port-level statistics. Keywords and arguments are as follows: • **all** --Statistics for all voice ports. • *voice-port-label* --Statistics for a specific voice port.
mode	(Optional) Statistics in a specified mode. Keywords are as follows: • concise--Output contains total calls, answered calls, and answered call duration. • verbose--All fields contained in call statistic records (CSRs). This is the default.
push	(Optional) Statistics are downloaded to an FTP or syslog server, or to both servers. Keywords are as follows: • all--Pushes statistics to both the FTP and syslog servers. • ftp--Pushes statistics to the FTP server. • syslog--Pushes statistics to the syslog server.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.3(4)T	This command was introduced.

Usage Guidelines

This command applies only if the **voice statistics time-range** command is configured to the **since-reset**value. Voice statistics collection on the gateway is reset using the **clear voice statistics csr**command.

If you enter the **show voice statistics csr since-reset aggregation-level** command but the gateway has been configured for periodic collection or to a specific interval, the gateway will display an error message.

Examples

The following sample output shows signaling statistics for all aggregation levels since the last reset:

```
Router# show voice statistics csr since-reset aggregation-level all
Client Type: VCSR
        Start Time: 2002-04-25T01:48:12Z        End Time: 2002-04-25T01:50:01Z
record_type=gw,trunk_group_id=,voice_port_id=,in_call=0,in_ans=0,in_fail=0,out_call=0,
out_ans=0,out_fail=0,in_szre_d=0,out_szre_d=0,in_conn_d=0,out_conn_d=0,orig_disconn=0,
in_ans_abnorm=0,out_ans_abnorm=0,in_mcd=0,out_mcd=0,in_pdd=0,out_pdd=0,in_setup_delay=0,
out_setup_delay=0,lost_pkt=0,latency=0,jitter=0,in_disc_cc_16=0,out_disc_cc_16=0
!
record_type=ip,trunk_group_id=,voice_port_id=,in_call=0,in_ans=0,in_fail=0,out_call=0,
out_ans=0,out_fail=0,in_szre_d=0,out_szre_d=0,in_conn_d=0,out_conn_d=0,orig_disconn=0,
in_ans_abnorm=0,out_ans_abnorm=0,in_mcd=0,out_mcd=0,in_pdd=0,out_pdd=0,in_setup_delay=0,
out_setup_delay=0,lost_pkt=0,latency=0,jitter=0,in_disc_cc_16=0,out_disc_cc_16=0
!
record_type=pstn,trunk_group_id=,voice_port_id=,in_call=0,in_ans=0,in_fail=0,out_call=0,
out_ans=0,out_fail=0,in_szre_d=0,out_szre_d=0,in_conn_d=0,out_conn_d=0,orig_disconn=0,
in_ans_abnorm=0,out_ans_abnorm=0,in_mcd=0,out_mcd=0,in_pdd=0,out_pdd=0,in_setup_delay=0,
out_setup_delay=0,in_disc_cc_16=0,out_disc_cc_16=0
!
record_type=vp,trunk_group_id=,voice_port_id=4/0/0,in_call=0,in_ans=0,in_fail=0,
out_call=0,out_ans=0,out_fail=0,in_szre_d=0,out_szre_d=0,in_conn_d=0,out_conn_d=0,
orig_disconn=0,in_ans_abnorm=0,out_ans_abnorm=0,in_mcd=0,out_mcd=0,in_pdd=0,out_pdd=0,
in_setup_delay=0,out_setup_delay=0,in_disc_cc_16=0,out_disc_cc_16=0
!
record_type=vp,trunk_group_id=,voice_port_id=4/0/1,in_call=0,in_ans=0,in_fail=0,
out_call=0,out_ans=0,out_fail=0,in_szre_d=0,out_szre_d=0,in_conn_d=0,out_conn_d=0,
orig_disconn=0,in_ans_abnorm=0,out_ans_abnorm=0,in_mcd=0,out_mcd=0,in_pdd=0,out_pdd=0,
in_setup_delay=0,out_setup_delay=0,in_disc_cc_16=0,out_disc_cc_16=0
!
record_type=vp,trunk_group_id=,voice_port_id=4/1/0,in_call=0,in_ans=0,in_fail=0,
out_call=0,out_ans=0,out_fail=0,in_szre_d=0,out_szre_d=0,in_conn_d=0,out_conn_d=0,
orig_disconn=0,in_ans_abnorm=0,out_ans_abnorm=0,in_mcd=0,out_mcd=0,in_pdd=0,out_pdd=0,
in_setup_delay=0,out_setup_delay=0,in_disc_cc_16=0,out_disc_cc_16=0
!
record_type=vp,trunk_group_id=,voice_port_id=4/1/1,in_call=0,in_ans=0,in_fail=0,
out_call=0,out_ans=0,out_fail=0,in_szre_d=0,out_szre_d=0,in_conn_d=0,out_conn_d=0,
orig_disconn=0,in_ans_abnorm=0,out_ans_abnorm=0,in_mcd=0,out_mcd=0,in_pdd=0,out_pdd=0,
in_setup_delay=0,out_setup_delay=0,in_disc_cc_16=0,out_disc_cc_16=0
!
record_type=vp,trunk_group_id=,voice_port_id=2/0:23,in_call=0,in_ans=0,in_fail=0
,out_call=0,out_ans=0,out_fail=0,in_szre_d=0,out_szre_d=0,in_conn_d=0,out_conn_d=0,
orig_disconn=0,in_ans_abnorm=0,out_ans_abnorm=0,in_mcd=0,out_mcd=0,in_pdd=0,out_pdd=0,
in_setup_delay=0,out_setup_delay=0,in_disc_cc_16=0,out_disc_cc_16=0
!
record_type=vp,trunk_group_id=,voice_port_id=2/1:23,in_call=0,in_ans=0,in_fail=0
out_call=0,out_ans=0,out_fail=0,in_szre_d=0,out_szre_d=0,in_conn_d=0,out_conn_d=0,
orig_disconn=0,in_ans_abnorm=0,out_ans_abnorm=0,in_mcd=0,out_mcd=0,in_pdd=0,out_pdd=0,
in_setup_delay=0,out_setup_delay=0,in_disc_cc_16=0,out_disc_cc_16=0
```

The following sample output shows signaling statistics for the IP aggregation level since the last reset:

```
Router# show voice statistics csr since-reset aggregation-level ip
Client Type: VCSR
```

```
        Start Time: 2002-04-25T01:48:12Z        End Time: 2002-05-02T21:21:27Z
record_type=ip,trunk_group_id=10,voice_port_id=2,in_call=15,in_ans=15,in_fail=0,out_call=0,out_ans=0,out_fail=0,in_szre_d=0,out_szre_d=0,in_conn_d=0,out_conn_d=0,orig_disconn=0,
in_ans_abnorm=0,out_ans_abnorm=0,in_mcd=0,out_mcd=0,in_pdd=0,out_pdd=0,in_setup_delay=0,
out_setup_delay=0,lost_pkt=0,latency=0,jitter=0,in_disc_cc_16=0,out_disc_cc_16=0
```

The following sample output shows signaling statistics for the PSTN aggregation level since the last reset:

```
Router# show voice statistics csr since-reset aggregation-level pstn
Client Type: VCSR
        Start Time: 2002-04-25T01:48:12Z        End Time: 2002-05-02T21:21:42Z
record_type=pstn,trunk_group_id=25,voice_port_id=2,in_call=100,in_ans=10,in_fail=90,
out_call=0,out_ans=0,out_fail=0,in_szre_d=100,out_szre_d=0,in_conn_d=0,out_conn_d=0,
orig_disconn=0,in_ans_abnorm=0,out_ans_abnorm=0,in_mcd=0,out_mcd=0,in_pdd=0,out_pdd=0,
in_setup_delay=0,out_setup_delay=0,in_disc_cc_16=0,out_disc_cc_16=0
```

The table below lists and describes the significant output fields.

Table 195: show voice statistics csr since-reset aggregation-level Field Descriptions

Field	Description
Client Type	The type of statistics collected.
Start Time	The start time of the statistics collection.
End Time	The ending time of the statistics collection.
record_type	Call statistics record type. Symbols are gw, ip, pstn, tg, and vp.
trunk_group_id	Trunk group ID. **Note** For the symbols gw, ip, pstn, and some vp records, this field is empty.
voice_port_id	Voice port ID. **Note** For the symbols gw, ip, pstn, and some vp records, this field is empty.
in_call	Number of incoming calls.
in_ans	Number of incoming calls answered by the gateway.
in_fail	Number of incoming calls that failed.
out_call	Number of outgoing calls attempted.
out_ans	Number of outgoing calls that received answers.
out_fail	Number of outgoing calls that failed.
in_szre_d	Incoming seizure duration (in seconds).
out_szre_d	Outgoing seizure duration (in seconds).
in_conn_d	Incoming connected duration (in seconds).

Field	Description
out_conn_d	Outgoing connected duration (in seconds).
orig_disconn	Number of calls encountering the originating side having been disconnected before the outgoing calls were connected.
in_ans_abnorm	Number of incoming answered calls terminated with any cause code other than "normal".
out_ans_abnorm	Number of outgoing answered calls terminated with any cause code other than "normal".
in_mcd	Number of incoming calls lasting less than the configured minimum call duration (MCD).
out_mcd	Number of outgoing calls lasting less than the configured MCD.
in_pdd	Total post dial delay duration on incoming calls (in ms).
out_pdd	Total post dial delay duration on outgoing calls (in ms).
in_setup_delay	Total inbound setup delay duration (in ms).
out_setup_delay	Total outbound setup delay duration (in ms).
lost_pkt	Number of calls losing more than the configured number of packets. **Note** This field will exist only in IP records. In other types of records, this field will be empty and extra commas are expected.
latency	Number of calls encountering more than the configured amount of latency. **Note** This field will exist only in "IP" records. In other types of records, this field will be empty and extra commas are expected.
jitter	Number of calls encountering more than configured amount of jitter. **Note** This field will exist only in IP records. In other types of records, this field will be empty and extra commas are expected.
in_disc_cc	Incoming disconnect cause code. For example, in_disc_cc_16=3 indicates that 3 calls were disconnected or finished with a disconnect cause code of 16 (normal).
out_disc_cc	Outgoing disconnect cause code.
in_cc_no	Number of the following disconnect cause code counters as per incoming calls (expected to be fewer than 5).
out_cc_no	Number of the following disconnect cause code counters as per outgoing calls (expected to be fewer than 5).
in_cc_id	Disconnect cause code ID for the following field for incoming calls.
in_cc_cntr	Disconnect cause code counter for incoming calls (any incoming cause code counter pairs).

Field	Description
out_cc_id	Disconnect cause code ID for the following field for outgoing calls.
out_cc_cntr	Disconnect cause code counter for outgoing calls (any outgoing cause code counter pairs).

Related Commands

Command	Description
clear voice statistics	Clears voice statistics, resetting the statistics collection.
clear voice statistics csr	Clears voice-statistic collection settings on the gateway.
show event-manager consumers	Displays event statistics.
show voice statistics csr interval accounting	Displays statistical information by configured intervals for accounting statistics.
show voice statistics csr interval aggregation	Displays statistical information by configured intervals for signaling statistics.
show voice statistics csr since-reset accounting	Displays all accounting CSRs since the last reset.
show voice statistics interval-tag	Displays voice statistics within a specified interval.
show voice statistics memory-usage	Displays current memory usage.
voice statistics time-range	Specifies the time range to collect CSRs.

show voice statistics csr since-reset all

To display all voice call statistical information since a reset occurred, use the **show voice statistics** csr since-reset all command in privileged EXEC mode.

show voice statistics csr since-reset all [**mode** {**concise** | **verbose**}] [**push** {**all** | **ftp** | **syslog**}]

Syntax Description

mode	(Optional) Statistics are displayed in a specified mode. The keywords are as follows: • concise--Displays output that contains total calls, answered calls, and answered call duration. • verbose--Displays all fields contained in call statistic records (CSRs). This is the default setting.
push	(Optional) Statistics are downloaded to an FTP or syslog server, or to both servers. The keywords are as follows: • all--Pushes statistics to both the FTP and syslog servers. • ftp--Pushes statistics to the FTP server. • syslog--Pushes statistics to the syslog server.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.3(4)T	This command was introduced.

Usage Guidelines

This command can also be used to display and push VoIP internal error codes (IECs).

Examples

The following example shows all of the statistics that were collected since the last reset:

```
Router# show voice statistics csr since-reset all
Client Type: VCSR
        Start Time: 2002-05-01T19:35:17Z        End Time: 2002-05-01T19:36:26Z
record_type=gw,trunk_group_id=,voice_port_id=,in_call=0,in_ans=0,in_fail=0,out_call=0,
out_ans=0,out_fail=0,in_szre_d=0,out_szre_d=0,in_conn_d=0,out_conn_d=0,orig_disconn=0,
in_ans_abnorm=0,out_ans_abnorm=0,in_mcd=0,out_mcd=0,in_pdd=0,out_pdd=0,in_setup_delay=0,
out_setup_delay=0,lost_pkt=0,latency=0,jitter=0,in_disc_cc_16=0,out_disc_cc_16=0
!
record_type=ip,trunk_group_id=,voice_port_id=,in_call=0,in_ans=0,in_fail=0,out_call=0,
out_ans=0,out_fail=0,in_szre_d=0,out_szre_d=0,in_conn_d=0,out_conn_d=0,orig_disconn=0,
in_ans_abnorm=0,out_ans_abnorm=0,in_mcd=0,out_mcd=0,in_pdd=0,out_pdd=0,in_setup_delay=0,
out_setup_delay=0,lost_pkt=0,latency=0,jitter=0,in_disc_cc_16=0,out_disc_cc_16=0
!
record_type=pstn,trunk_group_id=,voice_port_id=,in_call=0,in_ans=0,in_fail=0,out_call=0,
out_ans=0,out_fail=0,in_szre_d=0,out_szre_d=0,in_conn_d=0,out_conn_d=0,orig_disconn=0,
in_ans_abnorm=0,out_ans_abnorm=0,in_mcd=0,out_mcd=0,in_pdd=0,out_pdd=0,in_setup_delay=0,
out_setup_delay=0,in_disc_cc_16=0,out_disc_cc_16=0
!
record_type=vp,trunk_group_id=,voice_port_id=4/0/0,in_call=0,in_ans=0,in_fail=0,
out_call=0,out_ans=0,out_fail=0,in_szre_d=0,out_szre_d=0,in_conn_d=0,out_conn_d=0,
```

```
orig_disconn=0,in_ans_abnorm=0,out_ans_abnorm=0,in_mcd=0,out_mcd=0,in_pdd=0,out_pdd=0,
in_setup_delay=0,out_setup_delay=0,in_disc_cc_16=0,out_disc_cc_16=0
!
record_type=vp,trunk_group_id=,voice_port_id=4/0/1,in_call=0,in_ans=0,in_fail=0,
out_call=0,out_ans=0,out_fail=0,in_szre_d=0,out_szre_d=0,in_conn_d=0,out_conn_d=0,
orig_disconn=0,in_ans_abnorm=0,out_ans_abnorm=0,in_mcd=0,out_mcd=0,in_pdd=0,out_pdd=0,
in_setup_delay=0,out_setup_delay=0,in_disc_cc_16=0,out_disc_cc_16=0
!
record_type=vp,trunk_group_id=,voice_port_id=4/1/0,in_call=0,in_ans=0,in_fail=0,
out_call=0,out_ans=0,out_fail=0,in_szre_d=0,out_szre_d=0,in_conn_d=0,out_conn_d=0,
orig_disconn=0,in_ans_abnorm=0,out_ans_abnorm=0,in_mcd=0,out_mcd=0,in_pdd=0,out_pdd=0,
in_setup_delay=0,out_setup_delay=0,in_disc_cc_16=0,out_disc_cc_16=0
!
record_type=vp,trunk_group_id=,voice_port_id=4/1/1,in_call=0,in_ans=0,in_fail=0,
out_call=0,out_ans=0,out_fail=0,in_szre_d=0,out_szre_d=0,in_conn_d=0,out_conn_d=0,
orig_disconn=0,in_ans_abnorm=0,out_ans_abnorm=0,in_mcd=0,out_mcd=0,in_pdd=0,out_pdd=0,
in_setup_delay=0,out_setup_delay=0,in_disc_cc_16=0,out_disc_cc_16=0
!
record_type=vp,trunk_group_id=,voice_port_id=2/0:23,in_call=0,in_ans=0,in_fail=0
out_call=0,out_ans=0,out_fail=0,in_szre_d=0,out_szre_d=0,in_conn_d=0,out_conn_d=0,
orig_disconn=0,in_ans_abnorm=0,out_ans_abnorm=0,in_mcd=0,out_mcd=0,in_pdd=0,out_pdd=0,
in_setup_delay=0,out_setup_delay=0,in_disc_cc_16=0,out_disc_cc_16=0
!
record_type=vp,trunk_group_id=,voice_port_id=2/1:23,in_call=0,in_ans=0,in_fail=0
out_call=0,out_ans=0,out_fail=0,in_szre_d=0,out_szre_d=0,in_conn_d=0,out_conn_d=0,
orig_disconn=0,in_ans_abnorm=0,out_ans_abnorm=0,in_mcd=0,out_mcd=0,in_pdd=0,out_pdd=0,
in_setup_delay=0,out_setup_delay=0,in_disc_cc_16=0,out_disc_cc_16=0
Client Type: Voice ACCT Stats
        Start Time: 2002-05-01T19:35:17Z        End Time: 2002-05-01T19:36:29Z
methodlist=h323-1,acc_pass_criteria=1,pstn_in_pass=0,pstn_in_fail=0,pstn_out_pass=0,
pstn_out_fail=0,ip_in_pass=0,ip_in_fail=0,ip_out_pass=0,ip_out_fail=0
```

The table below lists and describes the significant output fields.

Table 196: show voice statistics csr since-reset all Field Descriptions

Field	Description
Client Type	The type of statistics collected.
Start Time	The start time of the statistics collection.
End Time	The ending time of the statistics collection.
record_type	Call statistics record type. Symbols are gw, ip, pstn, tg, and vp.
trunk_group_id	Trunk group ID. **Note** For the symbols gw, ip, pstn, and some vp records, this field is empty.
voice_port_id	Voice port ID. **Note** For the symbols gw, ip, pstn, and some vp records, this field is empty.
in_call	Number of incoming calls.
in_ans	Number of incoming calls answered by the gateway.

Field	Description
in_fail	Number of incoming calls that failed.
out_call	Number of outgoing calls attempted.
out_ans	Number of outgoing calls that received answers.
out_fail	Number of outgoing calls that failed.
in_szre_d	Incoming seizure duration (in seconds).
out_szre_d	Outgoing seizure duration (in seconds).
in_conn_d	Incoming connected duration (in seconds).
out_conn_d	Outgoing connected duration (in seconds).
orig_disconn	Number of calls encountering the originating side having been disconnected before the outgoing calls were connected.
in_ans_abnorm	Number of incoming answered calls terminated with any cause code other than "normal".
out_ans_abnorm	Number of outgoing answered calls terminated with any cause code other than "normal".
in_mcd	Number of incoming calls lasting less than the configured minimum call duration (MCD).
out_mcd	Number of outgoing calls lasting less than the configured MCD.
in_pdd	Total post dial delay duration on incoming calls (in ms).
out_pdd	Total post dial delay duration on outgoing calls (in ms).
in_setup_delay	Total inbound setup delay duration (in ms).
out_setup_delay	Total outbound setup delay duration (in ms).
lost_pkt	Number of calls losing more than the configured number of packets. **Note** This field will exist only in IP records. In other types of records, this field will be empty and extra commas are expected.
latency	Number of calls encountering more than the configured amount of latency. **Note** This field will exist only in IP records. In other types of records, this field will be empty and extra commas are expected.
jitter	Number of calls encountering more than the configured amount of jitter. **Note** This field will exist only in IP records. In other types of records, this field will be empty and extra commas are expected.

Field	Description
in_disc_cc	Incoming disconnect cause code. For example, in_disc_cc_16=3 indicates that 3 calls were disconnected or finished with a disconnect cause code of 16 (normal).
out_disc_cc	Outgoing disconnect cause code.
in_cc_no	Number of the following disconnect cause code counters as per incoming calls (expected to be fewer than 5).
out_cc_no	Number of the following disconnect cause code counters as per outgoing calls (expected to be fewer than 5).
in_cc_id	Disconnect cause code ID for the following field for incoming calls.
in_cc_cntr	Disconnect cause code counter for incoming calls (any incoming cause code counter pairs).
out_cc_id	Disconnect cause code ID for the following field for outgoing calls.
out_cc_cntr	Disconnect cause code counter for outgoing calls (any outgoing cause code counter pairs).

Related Commands

Command	Description
clear voice statistics	Clears voice statistics, resetting the statistics collection.
show event-manager consumers	Displays event statistics.
show voice statistics csr interval accounting	Displays statistical information by configured intervals for accounting statistics.
show voice statistics csr interval aggregation	Displays statistical information by configured intervals for signaling statistics.
show voice statistics csr since-reset accounting	Displays all accounting CSRs since the last reset.
show voice statistics csr since-reset aggregation-level	Displays all signaling CSRs since the last reset.
show voice statistics interval-tag	Displays voice statistics within a specified interval.
show voice statistics memory-usage	Displays current memory usage.

show voice statistics iec

To display Internal Error Code (IEC) statistics, use the **show voice statistics iec** command in user EXEC or privileged EXEC mode.

show voice statistics iec {**interval** *number* | **since-reboot** | **since-reset**} [**push** [**all** | **ftp** | **syslog**]]

Syntax Description

interval	Displays statistics for the specified interval.
number	The interval tag number. The range is from 1 to 36655.
since-reboot	Displays IEC statistics since the last reboot.
since-reset	Displays IEC statistics since the last reset.
push	Specifies the off-load pushing interface.
all	Indicates that IEC statistics will be off-loaded to all push interfaces.
ftp	Indicates that IEC statistics will be off-loaded to the FTP server.
syslog	Indicates that IEC statistics will be off-loaded to the syslog server.

Command Modes

User EXEC (#)
Privileged EXEC(#)

Command History

Release	Modification
12.3(4)T	This command was introduced.
12.4(24)T	This command was modified in a release earlier than Cisco IOS Release 12.4(24)T. The **push all**, **ftp** and **syslog** keywords were added.

Usage Guidelines

Before you can display IEC statistics for a specific interval, use the **show voice statistics interval-tag** command to display available interval options. Before you display view IEC statistics since reboot, you must configure the **voice statistics type iec** command. Before you can display IEC statistics since the last reset, you must configure the **voice statistics type iec** command and the **voice statistics time-range since-reset** command.

Examples

The following is sample output from the **show voice statistics iec since-reset** command, which displays statistics since the last instance when IEC counters were cleared:

```
Router# show voice statistics iec since-reset
Internal Error Code counters
----------------------------
Counters since last reset (2002-11-28T01:55:31Z):
  SUBSYSTEM CCAPI [subsystem code 1]
      [errcode   6] No DSP resource                              5
  SUBSYSTEM SSAPP [subsystem code 4]
      [errcode   5] No dial peer match                           2
      [errcode   3] CPU high                                    96
```

```
SUBSYSTEM H323 [subsystem code 5]
    [errcode  22] No Usr Responding, H225 timeout            1
    [errcode 27] H225 invalid msg                           1
    [errcode 79] H225 chn, sock fail                       27
SUBSYSTEM VTSP [subsystem code 9]
    [errcode   6] No DSP resource                           83
```

The table below describes the significant fields shown in the display.

Table 197: show voice statistics iec Field Descriptions

Field	Description
SUBSYSTEM	Indicates the specific subsystem within the physical entity where the IEC was generated.
errcode	Identifies the error code within the subsystem.

The following is sample output from the **show voice statistics iec since-reset push all** command, which displays statistics since the last instance when IEC counters were cleared and off-loaded to all push interfaces.

```
Router# show voice statistics iec since-reset push all
Internal Error Code counters
----------------------------
Counters since last reset (2009-07-16T01:40:59Z):
No errors.
Router#
*Jul 16 01:43:39.530: %VSTATS-6-IEC: SEQ=1:
stats_type,version,entity_id,start_time,end_time,record_count
IEC,1,7206-2,2009-07-16T01:40:59Z,2009-07-16T01:43:39Z,0
```

Related Commands

Command	Description
clear voice statistics	Clears voice statistics, resetting the statistics collection.
show voice statistics	Displays voice statistics.
show voice statistics interval-tag	Displays interval options available for IEC statistics.
voice statistics time-range since-reset	Enables collection of call statistics accumulated since the last resetting of IEC counters.
voice statistics type iec	Enables collection of IEC statistics.

show voice statistics interval-tag

To display the interval numbers assigned by the gateway, use the **show voice statistics interval-tag** command in privileged EXEC mode.

show voice statistics interval-tag

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.3(4)T	This command was introduced.

Usage Guidelines

This is used to obtain the interval tag number required for the **show voice statistics csr interval accounting** and **show voice statistics csr interval aggregation** commands.

Examples

The following example shows the start and end times for specific interval tags:

```
Router# show voice statistics interval-tag
Current System Time is: 2002-4-1T010:10:00Z
 Interval-Tag    Intervals Start Time       End Time
 101    2002-3-31T010:00:00Z       2002-3-31T010:55:00Z
 105    2002-3-31T012:15:00Z       2002-3-31T012:30:00Z
```

The table below lists and describes the significant output fields.

Table 198: show voice statistics interval-tag Field Descriptions

Field	Description
Current System Time	Current system time of the gateway.
Interval-Tag	Interval number.
Intervals Start Time	Interval start time.
End Time	Interval end time.

Related Commands

Command	Description
show event-manager consumers	Displays event statistics.
show voice statistics csr interval accounting	Displays statistical information by configured intervals for accounting statistics.
show voice statistics csr interval aggregation	Displays statistical information by configured intervals for signaling statistics.

Command	Description
show voice statistics csr since-reset accounting	Displays all accounting CSRs since the last reset.
show voice statistics csr since-reset aggregation-level	Displays all signaling CSRs since the last reset.
show voice statistics csr since-reset all	Displays all CSRs since the last reset.
show voice statistics memory-usage	Displays current memory usage.

show voice statistics memory-usage

To display the memory used for collecting call statistics and to estimate the future use of memory, use the **show voice statistics memory-usage** command in privileged EXEC mode.

show voice statistics memory-usage {**all** | **csr** | **iec**}

Syntax Description

all	Memory used to collect both signaling and accounting call statistics records (CSRs).
csr	Memory used to collect signaling CSRs only.
iec	Memory used to collect Cisco internal error codes (IECs) only.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.3(4)T	This command was introduced.

Examples

The following example shows all of the memory used at a fixed interval and since the last reset for signaling and accounting; it also shows the estimated future memory to be used.

```
Router# show voice statistics memory-usage all
*** Voice Call Statistics Record Memory Usage ***
        Fixed Interval Option -
                CSR size: 136 bytes
                Number of CSR per interval: 9
                Used memory size (proximate): 0
                Estimated future claimed memory size (proximate): 0
        Since Reset Option -
                CSR size: 136 bytes
                Total count of CSR: 9
                Used memory size (proximate): 1224
*** Voice Call Statistics Accounting Record Memory Usage ***
        Fixed Interval Option -
                ACCT REC size: 80 bytes
                Number of ACCT REC per interval: 1
                Used memory size (proximate): 0
                Estimated future claimed memory size (proximate): 0
        Since Reset Option -
                ACCT REC size: 80 bytes
                Total count of ACCT REC: 1
                Used memory size (proximate): 80
```

The table below lists and describes the significant output fields.

Table 199: show voice statistics memory-usage Field Descriptions

Field	Description
Voice Call Statistics Record Memory Usage	

Field	Description
Fixed Interval Option:	Statistics gathered for a fixed interval.
CSR size	Size of the CSR for the fixed interval.
Number of CSR per interval	Number of CSRs collected for the fixed interval.
Used memory size (proximate)	Amount of memory currently being used to store statistics.
Estimated future claimed memory size (proximate)	Amount of remaining memory available to store statistics.
Since Reset Option:	Statistics gathered since the last reset or reboot of the gateway.
CSR size	Size of the CSR since the last reset.
Total count of CSR	Total number of CSRs gathered since the last reset.
Used memory size (proximate)	Amount of memory currently being used to store statistics.
Voice Call Statistics Accounting Record Memory Usage	
Fixed Interval Option:	Statistics gathered for a fixed interval.
ACCT REC size	Accounting record size.
Number of ACCT REC per interval	Number of accounting records per interval.
Used memory size (proximate)	Amount of memory currently being used to store statistics.
Estimated future claimed memory size (proximate)	Amount of remaining memory available to store statistics.
Since Reset Option:	Statistics gathered since the last reset or reboot of the gateway.
ACCT REC size	Accounting record size.
Total count of ACCT REC	Total number of accounting records since the last reset or reboot of the gateway.
Used memory size (proximate)	Amount of memory currently being used to store statistics.

Related Commands

Command	Description
show event-manager consumers	Displays event statistics.
show voice statistics csr interval accounting	Displays statistical information by configured intervals for accounting statistics.

Command	Description
show voice statistics csr interval aggregation	Displays statistical information by configured intervals for signaling statistics.
show voice statistics csr since-reset accounting	Displays all accounting CSRs since the last reset.
show voice statistics csr since-reset aggregation-level	Displays all signaling CSRs since the last reset.
show voice statistics csr since-reset all	Displays all CSRs since the last reset.
show voice statistics interval-tag	Displays the configured interval numbers.



show voice trace through shutdown (voice-port)

- show voice trace, on page 987
- show voice translation-profile, on page 988
- show voice translation-rule, on page 990
- show voice trunk-conditioning signaling, on page 992
- show voice trunk-conditioning supervisory, on page 995
- Show voice vrf, on page 998
- show voice vtsp, on page 999
- show voip debug version, on page 1001
- show voip fpi call-rate , on page 1002
- show voip fpi calls, on page 1003
- show voip fpi rtts, on page 1010
- show voip fpi stats, on page 1011
- show voip htsp, on page 1017
- show voip recmsp session, on page 1019
- show voip rtp connections, on page 1021
- show voip rtp forking, on page 1029
- show voip rtp stats, on page 1031
- show voip stream-service callid, on page 1035
- show voip stream-service connection, on page 1037
- show voip stream-service connection history, on page 1039
- show voip stream-service connection id, on page 1041
- show voip stream-service server, on page 1044
- show voip stream-service statistics , on page 1046
- show voip trace, on page 1048
- show voip trunk group, on page 1056
- show vrm active_calls, on page 1057
- show vrm vdevices, on page 1060
- show vsp, on page 1071
- show wsapi, on page 1076
- show xcsp port, on page 1080
- show xcsp slot, on page 1082
- shut, on page 1083
- shutdown (Annex G neighbor), on page 1084

- shutdown (Annex G), on page 1085
- shutdown (dial-peer), on page 1086
- shutdown (DSP Farm profile), on page 1087
- shutdown (gatekeeper), on page 1088
- shutdown (gateway), on page 1089
- shutdown (mediacard), on page 1090
- shutdown (auto-config application), on page 1091
- shutdown (RLM), on page 1092
- shutdown (settlement), on page 1093
- shutdown (trace), on page 1095
- shutdown (voice-port), on page 1097

show voice trace

To display the call trace information about a specified port, use the **show voice trace** command in privileged EXEC mode.

show voice trace *interface-slot* [**detail**]

Syntax Description

interface-slot	Voice interface slot.
detail	(Optional) Displays detailed statistics of the specified port.

Command Default

Privileged EXEC (#)

Command History

Release	Modification
15.0(1)M	This command was introduced in a release earlier than Cisco IOS Release 15.0(1)M.

Usage Guidelines

Use the **show voice trace** command to display the call trace information about specified port. The field descriptions are self-explanatory.

Examples

The following is sample output from the **show voice trace** command:

```
Router# show voice trace 1/1/1 detail

1/1/1 Stack 0:
State Transitions: timestamp (state, event) -> (state, event) ...
96.732 (S_OPEN_PEND, E_DSP_INTERFACE_INFO) ->
96.732 (S_DOWN, E_HTSP_IF_INSERVICE) ->
97.092 (S_OPEN_PEND, E_HTSP_GO_UP) ->
Event Counts (zeros not shown): (event, count)
(E_HTSP_IF_INSERVICE, 1) :(E_HTSP_GO_UP, 1) :(E_DSP_INTERFACE_INFO, 1) :
State Counts (zeros not shown): (state, count)
(S_OPEN_PEND, 2) :(S_DOWN, 1) :
Stack 1:
State Transitions: timestamp (state, event) -> (state, event) ...
97.092 (DID_NULL, E_DSP_SIG_0100) ->
97.092 (DID_INIT, E_HTSP_INSERVE) ->
97.092 (DID_PENDING, E_DSP_SIG_0100) ->
Event Counts (zeros not shown): (event, count)
(E_HTSP_INIT, 1) :(E_HTSP_INSERVE, 1) :(E_DSP_SIG_0100, 2) :
State Counts (zeros not shown): (state, count)
(DID_NULL, 2) :(DID_INIT, 1) :(DID_PENDING, 1) :
```

show voice translation-profile

To display one or more translation profiles, use the **show voice translation-profile** command in privileged EXEC mode.

show voice translation-profile [*name* | **sort** [**ascending** | **descending**]]

Syntax Description

name	Name of the translation profile to display.
sort [**ascending** | **descending**	Display order of the translation profiles by *name*.

Command Default

Ascending order

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.2(11)T	This command was introduced.

Examples

The following sample output displays all the voice translation profiles in ascending order:

```
Router# show voice translation-profile sort ascending
Translation Profile: 1
 Rule for Calling number:
 Rule for Called number: 1
 Rule for Redirect number:
Translation Profile: 2
 Rule for Calling number:1
 Rule for Called number: 2
 Rule for Redirect number:
Translation Profile: 6
 Rule for Calling number:1
 Rule for Called number: 6
 Rule for Redirect number:2
```

The table below describes the fields shown in this output.

Table 200: show voice translation-profile Field Descriptions

Field	Description
Translation Profile	Name of the translation profile.
Rule for Called number	Number of the rule used for translating called numbers. If the field is blank, this translation profile does not have a rule assigned to that number type.
Rule for Calling number	Number of the rule used for translating calling numbers. If the field is blank, this translation profile does not have a rule assigned to that number type.
Rule for Redirect number	Number of the rule used for translating redirect numbers. If the field is blank, this translation profile does not have a rule assigned to that number type.

Related Commands

Command	Description
voice translation-profile	Initiates a voice translation-profile definition.
voice translation-rule	Initiates a voice translation-rule definition.

show voice translation-rule

To display one or more translation rules, use the **show voice translation-rule** command in privileged EXEC mode.

show voice translation-rule [*number* | **sort** [**ascending** | **descending**]]

Syntax Description

number	Number of the translation rule to display. Valid values are from 1 to 2147483647.
sort [**ascending** | **descending**	Display order of the translation rules by *number*.

Command Default

Ascending order

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.2(11)T	This command was introduced.

Usage Guidelines

Under each translation rule are numbered subrules.

Examples

The following sample output displays the translation rule number 6:

```
Router# show voice translation-rule 6
Translation-rule tag: 6
   Rule 1:
   Match pattern: 65088801..
   Replace pattern: 6508880101
   Match type: none   Replace type: none
   Match plan: none   Replace plan: none
```

The following sample output displays all the translation rules in ascending order:

```
Router# show voice translation-rule sort ascending
Translation-rule tag: 1
   Rule 3:
   Match pattern: 5108880...
   Replace pattern: 5108880101
   Match type: none   Replace type: none
   Match plan: none   Replace plan: none
   Rule 4:
   Match pattern: 510890....
   Replace pattern: 5108880101
   Match type: none   Replace type: none
   Match plan: none   Replace plan: none
Translation-rule tag: 2
   Rule 1:
   Match pattern: 51088802..
   Replace pattern: 5108880101
   Match type: none   Replace type: none
   Match plan: none   Replace plan: none
```

```
Rule 2:
Match pattern: 51088803..
Replace pattern: 5108880101
Match type: none   Replace type: none
Match plan: none   Replace plan: none
Rule 3:
Match pattern: 510889....
Replace pattern: 5108880101
Match type: none  Replace type: none
Match plan: none   Replace plan: none
Rule 4:
Match pattern: 510890....
Replace pattern: 5108880101
Match type: none   Replace type: none
Match plan: none   Replace plan: none
```

The table below describes the fields shown in this output.

Table 201: show voice translation-rule Field Descriptions

Field	Description
Translation-rule tag	Number of the translation rule.
Rule	Number of the rule defined within the translation rule.
Match pattern	SED-like expression used to match incoming call information.
Replace pattern	SED-like expression used to replace *match-pattern* in the call information.
Match type	Type of incoming calls to match.
Replace type	Type to replace Match type.
Match plan	Plan of incoming calls to match.
Replace plan	Plan to replace Match plan.

Related Commands

Command	Description
rule (voice translation-rule)	Defines the SED expressions for translating calls.
test voice translation-rule	Tests the rules in a translation-rule definition.
voice translation-rule	Initiates a voice translation-rule definition.
voice translation-profile	Initiates a voice translation-profile definition.

show voice trunk-conditioning signaling

To display the status of trunk-conditioning signaling and timing parameters for a voice port, use the **show voice trunk-conditioning signaling** command in user EXEC or privileged EXEC mode.

show voice trunk-conditioning signaling [**summary***voice-port*]

Syntax Description

summary	(Optional) Displays a summary of the status for all voice ports on the router or concentrator.
voice -port	(Optional) Displays a detailed report for a specified voice port.

Command Modes

User EXEC (>)
Privileged EXEC (#)

Command History

Release	Modification
12.0(3)XG	This command was introduced on the Cisco MC3810 as the **show voice permanent-call** command.
12.0(4)T	This command was integrated into Cisco IOS Release 12.0(4)T.
12.0(7)XK	This command was renamed **show voice trunk-conditioning signaling**.
12.1(2)T	This command was integrated into Cisco IOS Release 12.1(2)T.
12.1(3)T	This command was implemented on the Cisco 2600 series and Cisco 3600 series.

Usage Guidelines

This command displays the trunk signaling status for analog and digital voice ports on the Cisco 2600 series and the Cisco 3600 series routers.

Examples

The following is sample output from the **show voice trunk-conditioning signaling summary** command:

```
Router# show voice trunk-conditioning signaling summary
2/0/0 is shutdown
2/0/1 is shutdown
3/0:0 8  is shutdown
3/0:1 1  is shutdown
3/0:2 2  is shutdown
3/0:3 3  is shutdown
3/0:5 5  is shutdown
3/0:6(6) :
 status :
3/0:7 7  is shutdown
3/1:0 8  is shutdown
3/1:1 1  is shutdown
3/1:3 3  is shutdown
3/1:5 5  is shutdown
3/1:7 7  is shutdown
```

The following is sample output from the **show voice trunk-conditioning signaling** command for voice port 3/0:6:

```
Router# show voice trunk-conditioning signaling 3/0:6
hardware-state ACTIVE signal type is NorthamericanCAS
status :
forced playout pattern = STOPPED
trunk_down_timer = 0, rx_ais_duration = 0, idle_timer = 0
```

The table below describes significant fields in these outputs.

Table 202: show voice trunk-conditioning signaling Field Descriptions

Field	Description
current timer	Time since last signaling packets were received.
forced playout pattern	Which forced playout pattern is sent to PBX: • 0 = no forced playout pattern is sent • 1 = receive IDLE playout pattern is sent • 2 = receive OOS playout pattern is sent
hardware-state	Hardware state based on received IDLE pattern: • IDLE = both sides are idle • ACTIVE = at least one side is active
signal type	Signaling type used by lower level driver: northamerica, melcas, transparent, or external.
idle timer	Time the hardware on both sides has been in idle state.
last-ABCD	Last received or transmitted signal bit pattern.
max inter-arrival time	Maximum interval between received signaling packets.
missing	Number of missed signal packets.
mode	Signaling packet generation frequency: • Fast mode = every 4 milliseconds • Slow mode = same frequency as keepalive timer
out of seq	Number of out-of-sequence signal packets.
playout depth	Number of packets in playout buffer.
prev-seq#	Sequence number of previous signaling packet.
refill count	Number of packets created to maintain nominal length of playout packet buffer.
rx_ais_duration	Time since receipt of AIS indicator.

Field	Description
seq#	Sequence number of signaling packet.
sig pkt cnt	Number of transmitted or received signaling packets.
signal path	Status of signaling path.
signaling playout history	Signaling bits received in last 60 milliseconds.
trunk_down_timer	Time since last signaling packets were received.
tx_oos_timer	Time since PBX started sending OOS signaling pattern defined by **signal pattern oos transmit**.
very late	Number of very late signaling packets.

Related Commands

Command	Description
show dial-peer voice	Displays the configuration for all VoIP and POTS dial peers configured on the router.
show voice dsp	Shows the current status of all DSP voice channels.
show voice port	Displays configuration information about a specific voice port.
show voice trunk-conditioning supervisory	Displays the status of trunk supervision and configuration parameters for voice ports.

show voice trunk-conditioning supervisory

To display the status of trunk supervision and configuration parameters for a voice port, use the **show voice trunk-conditioning supervisory** command in user EXEC or privileged EXEC mode.

show voice trunk-conditioning supervisory [**summary***voice-port*]

Syntax Description

summary	(Optional) Displays a summary of the status for all voice ports on the router or concentrator.
voice -port	(Optional) Detailed report for a specified voice port.

Command Modes

User EXEC (>)
Privileged EXEC (#)

Command History

Release	Modification
12.0(7)XK	This command was introduced on the Cisco 2600 series, Cisco 3600 series, and Cisco MC3810 platforms.
12.1(2)T	This command was integrated into Cisco IOS Release 12.1(2)T.
12.1(3)T	This command was implemented on the Cisco 2600 series and Cisco 3600 series.
12.4(15)T10	The output of thiscommand was modified to report values configured by the **signal timing idle suppress-voice** command. The values for the **suppress-voice** and **resume-voice** keywords are shown as the "idle = *seconds*" and "idle_off = *milliseconds*" fields, respectively.

Usage Guidelines

This command displays the trunk supervision and configuration status for analog and digital voice ports.

Examples

The following is sample output for the **show voice trunk-conditioning supervisory** command:

```
Router# show voice trunk-conditioning supervisory 0/2/00/2/0 : state : TRUNK_SC_PENDING_START,
 voice : on, signal : off,active
 status: trunk disconn
 sequence oos : idle and oos
 pattern :rx_idle = 0101 rx_oos = 1111
 timeout timing : idle = 0, idle_off = 0, restart = 0, standby = 0, timeout = 0
 supp_all = 0, supp_voice = 0, keep_alive = 5
 timer: oos_ais_timer = 0, timer = 3
```

The following is sample output for the **show voice trunk-conditioning supervisory** command for voice port 0/2/0:

```
Router# show voice trunk-conditioning supervisory 3/0:6
0/2/0 : state : TRUNK_SC_PENDING_START, voice : on, signal : off,active
 status: trunk disconn
 sequence oos : idle and oos
 pattern :rx_idle = 0101 rx_oos = 1111
 timeout timing : idle = 0, idle_off = 0, restart = 0, standby = 0, timeout = 0
```

```
 supp_all = 0, supp_voice = 0, keep_alive = 5
 timer: oos_ais_timer = 0, timer = 3
```

The following shows a sample trunk conditioning setting for the **voice class permanent** command and sample output from the **s how voice trunk-conditioning supervisory** command that shows the values for the timeout timing field:

```
!
voice class permanent 1
  signal pattern idle transmit 0101
  signal pattern idle receive 0101
  signal pattern oos transmit 1111
  signal pattern oos receive 0101
  signal timing idle suppress-voice 10 resume-voice 150
!
Router# show voice trunk-conditioning supervisory

SLOW SCAN
0/0/0:0(1) : state : TRUNK_SC_CONNECT, voice : off , signal : on ,inactive
 status: rcv IDLE, trunk connected
 sequence oos : idle and oos
 pattern :rx_idle = 0101 rx_oos = 0101 tx_idle = 0101 tx_oos =  1111
 timeout timing : idle = 10, idle_off = 150, restart = 0, standby = 0, timeout = 30
 supp_all = 0, supp_voice = 0, keep_alive = 5
 timer: oos_ais_timer = 0, timer = 0
```

The table below describes the significant fields shown in the display.

Table 203: show voice trunk-conditioning supervisory Field Descriptions

Field	Description
idle	Timer setting (in seconds) configured by the **suppress-voice** option of the **signal timing idle suppress-voice** command.
idle_off	Timer setting (in milliseconds) configured by the **resume-voice** option of the **signal timing idle suppress-voice** command.
keep_alive	Signaling packets periodically sent to the far end, even if there is no signal change. These signaling packets function as keep alive messages.
active	Voice port configured as "connect trunk *xxxx* ."
oos_ais_timer	Time since the signaling packet with alarm indication signal (AIS) indicator was received.
pattern	4-bit signaling pattern.
restart	Restart timeout after far end is out-of-service (OOS).
rx-idle	Signaling bit pattern indicating that the far end is idle.
rx-oos	Signaling bit pattern sent to the PBX indicating that the network is OOS.
standby	Time before the inactive side goes back to standby after the far end goes OOS.
supp_all	Timeout before suppressing transmission of voice and signaling packets to the far end after detection of PBX OOS.

Field	Description
supp_voice	Timeout before suppressing transmission of voice packet to the far end after detection of PBX OOS.
timeout	Timeout for nonreceipt of keepalive packets before the far end is considered to be OOS.
timeout timing	Delay between the detection of incoming seizure and when the digital signal processor (DSP)-to-Cisco IOS interaction to open up the audio path is initiated.
TRUNK_SC_CONNECT	Trunk conditioning supervisory component status.

Related Commands

Command	Description
show dial-peer voice	Displays the configuration for all VoIP and POTS dial peers configured on the router.
show voice dsp	Displays the current status of all DSP voice channels.
show voice port	Displays configuration information about a specific voice port.
show voice trunk-conditioning signaling	Displays the status of trunk-conditioning signaling and timing parameters for a voice port.
voice-class permanent	Assigns a previously configured voice class for a Cisco trunk or FRF.11 trunk to a voice port.

Show voice vrf

To display the voice VRF configured at global configuration level and IP VRF associated with the bind interface configured under global sip services mode. use **show voice vrf** command in privileged EXEC mode.

show voice vrf

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS 15.6(2)T	This command was introduced.
Cisco IOS XE Denali 16.3.1	This command was integrated into Cisco IOS XE Denali 16.3.1.

Usage Guidelines

Use this command to display information associated with VRF.

Example

If voice vrf VRF1 is configured at global configuration level and sip bind is configured with interface that has vrf id VRF2, then the output is as follows:

```
Device# show voice vrf

==========VOICE VRF CONFIGURATION==========

Global voice vrf defined is: VRF1
Global sip bind for vrf is: VRF2
```

If voice vrf VRF1 is configured and sip bind is configured with interface that is not assigned any vrf id, then the output is as follows:

```
Device# show voice vrf

==========VOICE VRF CONFIGURATION==========

Global voice vrf defined is: VRF1
Global sip bind for vrf is: NA
```

If both voice vrf and sip bind at global level is not configured, then the output is as follows:

```
Device# show voice vrf

==========VOICE VRF CONFIGURATION==========

Global voice vrf defined is: NA
Global sip bind for vrf is: NA
```

show voice vtsp

To display information about the voice port configuration and Voice Telephony Service Provider (VTSP), use the **show voice vtsp** command in privileged EXEC mode.

show voice vtsp {**call** [**dspstats** | **fsm** | **log** [*call-ID*] | **verbose**] | **fork dsp-status**} [*call ID*]

Syntax Description

call	Displays the call control block information.
dspstats	(Optional) Displays the selective statistics of digital signal processor (DSP) voice channels.
fsm	(Optional) Displays information about the Finite State Machine Dump (FSM).
log *call-ID*	(Optional) Displays the call related logs. If a call ID is specified, this command displays the status of a specific call. The call ID value range is from 1 to 4294967295
verbose	(Optional) Displays the verbose output.
fork	Displays the media forking information.
dsp-status	Displays the status of media forking in the DSP.
call-ID	(Optional) Displays the status of the call. The value range is from 0x0 to 0xFFFFFFFF. >

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.4(24)T	This command was introduced in a release earlier than Cisco IOS Release 12.4(24)T.

Usage Guidelines

Use the **show voice vtsp** command to display information about the voice port configuration.

Examples

The following is sample output from the **show voice vtsp** command:

```
Router# show voice vtsp call dspstats 0x833

***DSP VOICE TX STATISTICS***
Tx Vox/Fax Pkts: 1337, Tx Sig Pkts: 0, Tx Comfort Pkts: 181
Tx Dur(ms): 46840, Tx Vox Dur(ms): 26740, Tx Fax Dur(ms): 0
        ***DSP VOICE RX STATISTICS***
Rx Vox/Fax Pkts: 1347, Rx Signal Pkts: 0, Rx Comfort Pkts: 180
Rx Dur(ms): 46840, Rx Vox Dur(ms): 23300, Rx Fax Dur(ms): 0
Rx Non-seq Pkts: 0, Rx Bad Hdr Pkts: 0
Rx Early Pkts: 0, Rx Late Pkts: 0
        ***DSP VOICE VP_DELAY STATISTICS***
Clk Offset(ms): 80, Rx Delay Est(ms): 50
Rx Delay Lo Water Mark(ms): 50, Rx Delay Hi Water Mark(ms): 70
        ***DSP VOICE VP_ERROR STATISTICS***
Predict Conceal(ms): 0, Interpolate Conceal(ms): 0
Silence Conceal(ms): 0, Retroact Mem Update(ms): 0
Buf Overflow Discard(ms): 0, Talkspurt Endpoint Detect Err: 0
```

```
        ***DSP LEVELS***
TDM Bus Levels(dBm0): Rx -68.5 from PBX/Phone, Tx -4.4 to PBX/Phone
TDM ACOM Levels(dBm0): +64.1, TDM ERL Level(dBm0): +10.0
TDM Bgd Levels(dBm0): -80.0, with activity being silence
        ***DSP VOICE ERROR STATISTICS***
Rx Pkt Drops(Invalid Header): 0, Tx Pkt Drops(HPI SAM Overflow): 0
        ***DSP VOICE GSMAMR-NB STATISTICS***
EncodingRate: 7 DecodingRate: 7
numEncodeChanges: 0 numDecodeChanges: 0
numCRCFail: 0 numFrameBadQuality: 0
numInvalidCMR: 0 numInvalidFrameType: 0
```

Related Commands

Command	Description
debug vtsp	Displays the state of the gateway and the call events.

show voip debug version

To display the current version of the Voice over IP debug structure, use the **show voip debug version**command in privileged EXEC mode.

show voip debug version

Command Default

No default behavior or values

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.3(8)T	This command was introduced.

Examples

The following example shows output from the **show voip debug version** command:

```
Router# show voip debug version
voip debug version 1.0
```

The table below describes significant fields shown in the display.

Table 204: show voip debug version Field Descriptions

Field	Description
voip debug version 1.0	Shows the version of the debug structure.

Related Commands

Command	Description
show voip rtp connections	Displays RTP named event packets.

show voip fpi call-rate

To display the average call rates at the forwarding plane interface, use the **show voip fpi call-rate** command in privileged EXEC mode.

show voip fpi call-rate interval*seconds* **history** *seconds*

Syntax Description

interval	Displays the message rates at the FPI interface
seconds	The number of seconds for the interval. The range is from 1 to 300
history	Specifies how far back information is kept and displayed.
seconds	The number of seconds that will be displayed. The range is from 1 to 86400.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Release 3.9S	This command was introduced.

Usage Guidelines

This command displays the call-rate data that is collected on the forwarding plane interface when the **debug voip fpi call-rate** is enabled.

Example

The following shows the output for the **show voip fpi call-rate** command

```
Router# show voip fpi call-rate interval 1 history 1
------ ------ ------ ------ ------ ------ ------
Sec ADD MOD DEL EVT_UP EVT_DN CPU 5S
------ ------ ------ ------ ------ ------ ------
67 0 0 0 0 0 0
------ ------ ------ ------ ------ ------ ------
```

show voip fpi calls

To display call information for TDM and IVR calls in the Forwarding Plane Interface (FPI), use the **show voip fpi calls** command in privileged EXEC mode.

show voip fpi calls[**all** | **confID** *identifier* | **callID** *identifier* | **correlator** *identifier*]

Syntax Description

all	(Optional) Displays the detailed statistics for all calls in the FPI where the collection processes have been enabled.
confID *identifier*	(Optional) Displays detailed call information for a call at the application level.
callID *identifier*	(Optional) Displays detailed call information for a call based on the call ID.
correlator *identifier*	(Optional) Displays detailed call information for a call based on the correlator ID.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Release 3.9S	This command was introduced.
Cisco IOS XE Gibraltar 16.12.1a	The command output was enhanced to display the number of SRTP Rollover Counter (ROC) update events received from the data plane on per call basis.

Usage Guidelines

Call ID is a unique identifier for each call leg. Each call has the following two call legs:

- In Leg—The call coming in to CUBE.
- Out Leg—The call going out of CUBE.

Use **callID** *identifier* option to view the call leg details at the application level.

Conf ID is a unique identifier for a call (including both in leg and out leg) at the application level. Use **confID** *identifier* option to know the bridging details between in leg and out leg.

Correlator ID is a unique identifier for a call's (including both in leg and out leg) media session. Use **correlator** *identifier* option to view the media session details of a call.

Example

The following are sample output from the **show voip fpi calls** command

```
Router#show voip fpi calls
Number of Calls : 2
---------- ---------- ---------- ---------- --------------- ---------------
    confID correlator    AcallID     BcallID           state           event
---------- ---------- ---------- ---------- --------------- ---------------
        20         20         87         88       ALLOCATED DETAIL_STAT_RSP
        21         21         89         90       ALLOCATED DETAIL_STAT_RSP
```

```
Router#show voip fpi calls confID 20
--------------------------------------------------------------------------------
VoIP-FPI call entry details:
--------------------------------------------------------------------------------
Call Type        :        z    IP_IP     confID          :               20
correlator       :             20     call_state       :         ALLOCATED
last_event       :  DETAIL_STAT_RSP     alloc_start_time :       2737426765
modify_start_time:               0     delete_start_time:                0
Media Type(SideA):             RTP     Media Type(SideB):              RTP
--------------------------------------------------------------------------------
FPI State Machine Stats:
------------------------
create_req_call_entry_inserted             :         1
call_create_req_fsm_successful             :         1
call_provision_rsp_ok                      :         1
call_provision_rsp_fsm_successful          :         1
event_ind_media_up_to_app                  :         2
--------------------------------------------------------------------------------------------------------
SIDE_A  RTP details   -   gccb=0x7FE69FA11C08
--------------------------------------------------------------------------------------------------------
confID           :        20    fpi_user_data    :        20
callID           :        87    dstCallID        :        88    mainstcallID     :
87
srcport          :     16552    dstport          :     16580    DP add_sent      :
 1
dp_add_fail      :         0    dp_add_pending   :         0    dp_delete_sent   :
 0
dp_delete_waiting:         0    dp_delete_done   :         0    final_stats_pend :
 0
ha_create_sent   :         1    is_video         :         0    media_type       :
 0
is dspfarm xcode :        No    is conference    :        No    stream_type      :     VOICE
rtp_type         :  SENDRECV
--------------------------------------------------------------------------------------------------------
SIDE_B  RTP details   -   gccb=0x7FE6A9B5A960
--------------------------------------------------------------------------------------------------------
confID           :        20    fpi_user_data    :        20
callID           :        88    dstCallID        :        87    mainstcallID     :
88
srcport          :     16554    dstport          :     16400    DP add_sent      :
 1
dp_add_fail      :         0    dp_add_pending   :         0    dp_delete_sent   :
 0
dp_delete_waiting:         0    dp_delete_done   :         0    final_stats_pend :
 0
ha_create_sent   :         1    is_video         :         0    media_type       :
 0
is dspfarm xcode :        No    is conference    :        No    stream_type      :     VOICE
rtp_type         :  SENDRECV
--------------------------------------------------------------------------------------------------------
Detailed Stats from DataPlane:
------------------------------
mgm_handle      : 20
-----------------------------------------------------------------
Call Present in :    FMAN RP   FMAN FP       CPP
                  ---------------------------------------
                         YES       YES       YES
-----------------------------------------------------------------
                      Field               sideA               sideB
-----------------------------------------------------------------
          dtmf_payload_type                   0                   0
```

```
   redundant_data_pyld_type                 255                 255
                   tos_mask                   0                   0
                dtmf_flags                    0                   0
               ucode_flags                    5                   5
                local_port                16552               16554
           remote_port_tx                 16580               16400
           remote_port_rx                 16580               16400
               session_id           0x30000050          0x30000052
  hairpin_prtnr_null(ucode)                NULL                NULL
       hairpin_prtnr_callid                   0                   0
         dsp_interface_null                NULL                NULL
-----------------------------------------------------------------------

 DSP Resource Used : No
```

```
Router#show voip fpi calls callid 87
-------------------------------------------------------------------------------
VoIP-FPI call entry details:
-------------------------------------------------------------------------------
Call Type        :            IP_IP     confID           :              20
correlator       :               20     call_state       :       ALLOCATED
last_event       :  DETAIL_STAT_RSP     alloc_start_time :      2737426765
modify_start_time:                0     delete_start_time:               0
Media Type(SideA):              RTP     Media Type(SideB):             RTP
-------------------------------------------------------------------------------
FPI State Machine Stats:
------------------------
create_req_call_entry_inserted             :        1
call_create_req_fsm_successful             :        1
call_provision_rsp_ok                      :        1
call_provision_rsp_fsm_successful          :        1
event_ind_media_up_to_app                  :        2
-------------------------------------------------------------------------------------------------
SIDE_A  RTP details   -   gccb=0x7FE69FA11C08
-------------------------------------------------------------------------------------------------
confID           :        20    fpi_user_data    :        20
callID           :        87    dstCallID        :        88    mainstcallID     :
87
srcport          :     16552    dstport          :     16580    DP add_sent      :
 1
dp_add_fail      :         0    dp_add_pending   :         0    dp_delete_sent   :
 0
dp_delete_waiting:         0    dp_delete_done   :         0    final_stats_pend :
 0
ha_create_sent   :         1    is_video         :         0    media_type       :
 0
is dspfarm xcode :        No    is conference    :        No    stream_type      :     VOICE
rtp_type         :  SENDRECV
-------------------------------------------------------------------------------------------------
SIDE_B  RTP details   -   gccb=0x7FE6A9B5A960
-------------------------------------------------------------------------------------------------
confID           :        20    fpi_user_data    :        20
callID           :        88    dstCallID        :        87    mainstcallID     :
88
srcport          :     16554    dstport          :     16400    DP add_sent      :
 1
dp_add_fail      :         0    dp_add_pending   :         0    dp_delete_sent   :
 0
dp_delete_waiting:         0    dp_delete_done   :         0    final_stats_pend :
 0
ha_create_sent   :         1    is_video         :         0    media_type       :
 0
```

```
is dspfarm xcode :        No    is conference    :        No    stream_type      :     VOICE
rtp_type         :  SENDRECV
-------------------------------------------------------------------------------------------------
Detailed Stats from DataPlane:
------------------------------
mgm_handle      : 20
-------------------------------------------------------------------
Call Present in :    FMAN RP   FMAN FP       CPP
                    ----------------------------------------
                          YES       YES       YES
-------------------------------------------------------------------
                      Field              sideA               sideB
-------------------------------------------------------------------
          dtmf_payload_type                  0                   0
   redundant_data_pyld_type                255                 255
                   tos_mask                  0                   0
                dtmf_flags                   0                   0
               ucode_flags                   5                   5
                local_port               16552               16554
            remote_port_tx               16580               16400
            remote_port_rx               16580               16400
                session_id          0x30000050          0x30000052
  hairpin_prtnr_null(ucode)                NULL                NULL
       hairpin_prtnr_callid                  0                   0
         dsp_interface_null                NULL                NULL
-------------------------------------------------------------------

 DSP Resource Used : No


Router#show voip fpi calls all

Number of Calls : 2
---------------------------------------------------------------------------
VoIP-FPI call entry details:
---------------------------------------------------------------------------
Call Type        :            IP_IP     confID          :              24
correlator       :               24     call_state      :       ALLOCATED
last_event       :  DETAIL_STAT_RSP     alloc_start_time :      2902404766
modify_start_time:                0     delete_start_time:               0
Media Type(SideA):              RTP     Media Type(SideB):             RTP
---------------------------------------------------------------------------
FPI State Machine Stats:
------------------------
create_req_call_entry_inserted             :        1
call_create_req_fsm_successful             :        1
call_provision_rsp_ok                      :        1
call_provision_rsp_fsm_successful          :        1
event_ind_media_up_to_app                  :        2
-------------------------------------------------------------------------------------------------
SIDE_A  RTP details   -   gccb=0x7FE69FA11C08
-------------------------------------------------------------------------------------------------
confID           :        24    fpi_user_data    :        24
callID           :        95    dstCallID        :        96    mainstcallID     :
95
srcport          :     16568    dstport          :     16580    DP add_sent      :
 1
dp_add_fail      :         0    dp_add_pending   :         0    dp_delete_sent   :
 0
dp_delete_waiting:         0    dp_delete_done   :         0    final_stats_pend :
 0
ha_create_sent   :         1    is_video         :         0    media_type       :
 0
```

```
is dspfarm xcode :        No    is conference    :        No    stream_type      :     VOICE
rtp_type         :  SENDRECV
-------------------------------------------------------------------------------------------
SIDE_B  RTP details   -   gccb=0x7FE6A9B5A960
-------------------------------------------------------------------------------------------
confID           :        24    fpi_user_data    :        24
callID           :        96    dstCallID        :        95    mainstcallID     :
96
srcport          :     16570    dstport          :     16400    DP add_sent      :
 1
dp_add_fail      :         0    dp_add_pending   :         0    dp_delete_sent   :
 0
dp_delete_waiting:         0    dp_delete_done   :         0    final_stats_pend :
 0
ha_create_sent   :         1    is_video         :         0    media_type       :
 0
is dspfarm xcode :        No    is conference    :        No    stream_type      :     VOICE
rtp_type         :  SENDRECV
-------------------------------------------------------------------------------------------
Detailed Stats from DataPlane:
------------------------------
mgm_handle      : 24
-----------------------------------------------------------------
Call Present in :    FMAN RP   FMAN FP       CPP
                  ---------------------------------------
                         YES       YES       YES
-----------------------------------------------------------------
                      Field               sideA               sideB
-----------------------------------------------------------------
          dtmf_payload_type                   0                   0
   redundant_data_pyld_type                 255                 255
                  tos_mask                   0                   0
                dtmf_flags                   0                   0
               ucode_flags                   5                   5
                local_port               16568               16570
            remote_port_tx               16580               16400
            remote_port_rx               16580               16400
                session_id          0x30000060          0x30000062
  hairpin_prtnr_null(ucode)                NULL                NULL
       hairpin_prtnr_callid                   0                   0
         dsp_interface_null                NULL                NULL
-----------------------------------------------------------------

 DSP Resource Used : No
-------------------------------------------------------------
-------------------------------------------------------------------------------
VoIP-FPI call entry details:
-------------------------------------------------------------------------------
Call Type        :            IP_IP     confID           :              25
correlator       :               25     call_state       :       ALLOCATED
last_event       :  DETAIL_STAT_RSP     alloc_start_time :      2902505765
modify_start_time:                0     delete_start_time:               0
Media Type(SideA):              RTP     Media Type(SideB):             RTP
-------------------------------------------------------------------------------
FPI State Machine Stats:
------------------------
create_req_call_entry_inserted              :         1
call_create_req_fsm_successful              :         1
call_provision_rsp_ok                       :         1
call_provision_rsp_fsm_successful           :         1
event_ind_media_up_to_app                   :         1
-------------------------------------------------------------------------------------------
SIDE_A  RTP details   -   gccb=0x7FE6A9B9CFA8
-------------------------------------------------------------------------------------------
```

```
confID           :        25    fpi_user_data    :        25
callID           :        97    dstCallID        :        98    mainstcallID     :
97
srcport          :     16572    dstport          :     16584    DP add_sent      :
 1
dp_add_fail      :         0    dp_add_pending   :         0    dp_delete_sent   :
 0
dp_delete_waiting:         0    dp_delete_done   :         0    final_stats_pend :
 0
ha_create_sent   :         0    is_video         :         0    media_type       :
 0
is dspfarm xcode :        No    is conference    :        No    stream_type      :     VOICE
rtp_type         :  SENDRECV
-------------------------------------------------------------------------------------------
SIDE_B  RTP details   -   gccb=0x7FE69FA132F8
-------------------------------------------------------------------------------------------
confID           :        25    fpi_user_data    :        25
callID           :        98    dstCallID        :        97    mainstcallID     :
98
srcport          :     16574    dstport          :     16404    DP add_sent      :
 1
dp_add_fail      :         0    dp_add_pending   :         0    dp_delete_sent   :
 0
dp_delete_waiting:         0    dp_delete_done   :         0    final_stats_pend :
 0
ha_create_sent   :         1    is_video         :         0    media_type       :
 0
is dspfarm xcode :        No    is conference    :        No    stream_type      :     VOICE
rtp_type         :  SENDRECV
-------------------------------------------------------------------------------------------
Detailed Stats from DataPlane:
------------------------------
mgm_handle      : 25
-----------------------------------------------------------------
Call Present in :    FMAN RP   FMAN FP       CPP
                  ---------------------------------------
                         YES       YES       YES
-----------------------------------------------------------------
                      Field               sideA               sideB
-----------------------------------------------------------------
          dtmf_payload_type                   0                   0
   redundant_data_pyld_type                 255                 255
                  tos_mask                   0                   0
                dtmf_flags                   0                   0
               ucode_flags                   0                   5
                local_port               16572               16574
            remote_port_tx               16584               16404
            remote_port_rx               16584               16404
                session_id          0x30000064          0x30000066
  hairpin_prtnr_null(ucode)                NULL                NULL
       hairpin_prtnr_callid                   0                   0
         dsp_interface_null                NULL                NULL
-----------------------------------------------------------------

 DSP Resource Used : No
```

Determine information for a call based on correlator ID

To know the correlator ID, run `show call active voice compact` command and determine the active calls and its associated callID from the output. Make a note of the desired callID and enter the same while executing `show voip fpi calls callID xx` command. The command output displays

the correlator ID associated with the desired call ID. Enter the correlator ID while executing `show voip fpi calls correlator ID` command to know the number of Rollover Counter (ROC) updates that have come from the data plane to the control plane for a specific call.

The following is a sample output of `show call active voice compact` command.

```
Router#show call active voice compact
<callID>  A/O FAX T<sec> Codec       type        Peer Address       IP R<ip>:<udp>
Total call-legs: 4
       212 ANS     T735   pass-throug VOIP        P5553001        1.2.111.4:8376   <<< CUBE
 leg1, the remote peer is 1.2.111.4:8376(5553001)
       213 ORG     T735   pass-throug VOIP        P5553101        1.2.111.6:18898  <<< CUBE
 leg2, the remote peer is 1.2.111.6:18898(5553101)
       214 ORG     T735   g711ulaw    VOIP        P      1.2.111.108:16904         <<<
software MTP leg1, the remote peer is 1.2.111.108:16904
       215 ORG     T735   g711ulaw    VOIP        P        1.2.111.4:8372          <<<
software MTP leg2, the remote peer is 1.2.111.4:8372
```

Select callID 214 from the output and enter it in the `show voip fpi calls callID xx` command as shown below:

```
Router#show voip fpi calls callID 214 | include correlator
correlator       :              102     call_state       :        ALLOCATED
```

Enter correlator ID as 102 while executing `show voip fpi calls correlator ID` command as shown below to know the number of Rollover Counter (ROC) updates that have come from the data plane to the control plane for a specific call.

```
Router#show voip fpi calls correlator 102 | inc event

last_event       :    GET_STATS_RSP     alloc_start_time :       1024243582

event_ind_srtp_roc_upd_to_app               :         4
```

show voip fpi rtts

To display maximum, minimum, average and histogram for round trip times for create, modify and delete requests from control plane to forwarding plane, use **show voip fpi rtts** command in privileged EXEC mode.

show voip fpi rtts

Syntax Description

This command has no arguments or keywords.

Command Default

No default behavior or values.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Release 3.9S	This command was introduced.

Usage Guidelines

Use **show voip fpi rtts** command in privileged EXEC mode to display maximum, minimum, average and histogram for round trip times for create, modify, and delete requests from control plane to forwarding plane.

Example

```
Router#show voip fpi rtts
---------- ---------- ---------- ---------- ------------
   command      count  avg(msec)  max(msec) over_thrshld
---------- ---------- ---------- ---------- ------------
     ALLOC          1         38         38            0
    MODIFY          0          0          0            0
    DELETE          1          8          8            0
---------- ---------- ---------- ---------- ------------

HISTOGRAM
---------- ---------- ---------- ----------
     msecs      ALLOC     MODIFY     DELETE
---------- ---------- ---------- ----------
<= 10               0          0          1
<= 40               1          0          0
```

show voip fpi stats

To display the TDM and IVR statistics and error counters in the Forwarding Plane Interface (FPI), use the **show voip fpi stats** command in privileged EXEC mode.

show voip fpi stats [**fsm**]

Syntax Description

fsm	(Optional) Displays the finite state machine (FSM) events.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Release 3.9S	This command was introduced.
Cisco IOS XE Gibraltar 16.12.1a	The command output was enhanced to display the number of SRTP Rollover Counter (ROC) update events received from the data plane.

The following is a sample output from the **show voip fpi stats** command:

```
Router#show voip fpi stats
**************** VOIP FPI STATS *********************
----------- ---------- ---------- ---------- ----------
type        ReqSuccess    ReqFail RspSuccess    RspFail
----------- ---------- ---------- ---------- ----------
caps                 1          0          1          0
init                 1          0          1          0
params               1          0        N/A        N/A
config               0          0          0          0          0(skip)
deact                0          0          0          0     0(wrong state)
port add             2          0        N/A        N/A
port delete          0          0        N/A        N/A
********************** ACTIVE ******************************
                        IDLE      ALLOCATING       ALLOCATED       MODIFYING
     CREATE_REQ              1               0               0               0
     MODIFY_REQ              0               0               1               0
     DELETE_REQ              0               0               0               0
  GET_STATS_REQ              0               0               0               0
    PROV_RSP_OK              0               1               0               1
  PROV_RSP_FAIL              0               0               0               0
     DELETE_RSP              0               0               0               0
  GET_STATS_RSP              0               0               0               0
  STATS_TMR_EXP              0               0               0               0
     TMR_EXPIRY              0               0               0               0
CREATE_STRM_REQ              0               0               0               0
MODIFY_STRM_REQ              0               0               0               0
DELETE_STRM_REQ              0               0               0               0
DETAIL_STAT_REQ              0               0               0               0
DETAIL_STAT_RSP              0               0               0               0
DT_STAT_TMR_EXP              0               0               0               0
                     DELETING  ALLOC_MOD_PEND MODIFY_MOD_PEND  DELETE_PENDING
     CREATE_REQ              0               0               0               0
     MODIFY_REQ              0               0               0               0
     DELETE_REQ              0               0               0               0
  GET_STATS_REQ              0               0               0               0
    PROV_RSP_OK              0               0               0               0
  PROV_RSP_FAIL              0               0               0               0
```

```
     DELETE_RSP               0               0               0               0
   GET_STATS_RSP              0               0               0               0
   STATS_TMR_EXP              0               0               0               0
      TMR_EXPIRY              0               0               0               0
CREATE_STRM_REQ               0               0               0               0
MODIFY_STRM_REQ               0               0               0               0
DELETE_STRM_REQ               0               0               0               0
DETAIL_STAT_REQ               0               0               0               0
DETAIL_STAT_RSP               0               0               0               0
DT_STAT_TMR_EXP               0               0               0               0
********************** END ACTIVE ****************************


********************** STANDBY ******************************
                         IDLE      ALLOCATING       ALLOCATED       MODIFYING
     CREATE_REQ              0               0               0               0
     MODIFY_REQ              0               0               0               0
     DELETE_REQ              0               0               0               0
   GET_STATS_REQ             0               0               0               0
     PROV_RSP_OK             0               0               0               0
   PROV_RSP_FAIL             0               0               0               0
      DELETE_RSP             0               0               0               0
   GET_STATS_RSP             0               0               0               0
   STATS_TMR_EXP             0               0               0               0
      TMR_EXPIRY             0               0               0               0
CREATE_STRM_REQ               0               0               0               0
MODIFY_STRM_REQ               0               0               0               0
DELETE_STRM_REQ               0               0               0               0
DETAIL_STAT_REQ               0               0               0               0
DETAIL_STAT_RSP               0               0               0               0
DT_STAT_TMR_EXP               0               0               0               0
                     DELETING  ALLOC_MOD_PEND MODIFY_MOD_PEND  DELETE_PENDING
     CREATE_REQ              0               0               0               0
     MODIFY_REQ              0               0               0               0
     DELETE_REQ              0               0               0               0
   GET_STATS_REQ             0               0               0               0
     PROV_RSP_OK             0               0               0               0
   PROV_RSP_FAIL             0               0               0               0
      DELETE_RSP             0               0               0               0
   GET_STATS_RSP             0               0               0               0
   STATS_TMR_EXP             0               0               0               0
      TMR_EXPIRY             0               0               0               0
CREATE_STRM_REQ               0               0               0               0
MODIFY_STRM_REQ               0               0               0               0
DELETE_STRM_REQ               0               0               0               0
DETAIL_STAT_REQ               0               0               0               0
DETAIL_STAT_RSP               0               0               0               0
DT_STAT_TMR_EXP               0               0               0               0
********************** END STANDBY ***************************


Correlators in use:1

Corrupted table error (alloc):0

Corrupted table error (delete):0
----------- ---------- ---------- ---------- ----------
            gccb/rtpNL pr gccb NL no gccb sd badConfIds
----------- ---------- ---------- ---------- ----------
call create          0          0          0          0
            add sent T entry Fail entry insr fsm Succss
----------- ---------- ---------- ---------- ----------
                     0          0          1          1
```

```
            fsm failed ent delete       fail
----------- ---------- ---------- ---------- ----------
                     0          0          0

            entry !pre fsm failed fsm Succss
----------- ---------- ---------- ---------- ----------
call modify          0          0          1
            entry !pre entry del  fsm failed fsm Succss
----------- ---------- ---------- ---------- ----------
call delete          0          0          0          0

---------------- ---------- ---------- ---------- ----------
                 gccb/rtpNL pr gccb NL no gccb sd badConfIds
---------------- ---------- ---------- ---------- ----------
LPBK call create          0          0          0          0
                 add sent T entry Fail entry insr fsm Succss
---------------- ---------- ---------- ---------- ----------
                          0          0          0          0
                 fsm failed ent delete       fail
---------------- ---------- ---------- ---------- ----------
                          0          0          0

                 entry !pre fsm failed fsm Succss
---------------- ---------- ---------- ---------- ----------
LPBK call modify          0          0          0
                 entry !pre entry del  fsm failed fsm Succss
---------------- ---------- ---------- ---------- ----------
LPBK call delete          0          0          0          0
---------------- ---------- ---------- ---------- ----------

---------------- ---------- ---------- ---------- ----------
                 gccb/rtpNL pr gccb NL no gccb sd badConfIds
---------------- ---------- ---------- ---------- ----------
STRM call create          0          0          0          0
                 add sent T entry Fail entry insr fsm Succss
---------------- ---------- ---------- ---------- ----------
                          0          0          0          0
                 fsm failed ent delete       fail
---------------- ---------- ---------- ---------- ----------
                          0          0          0

                 entry !pre fsm failed fsm Succss
---------------- ---------- ---------- ---------- ----------
STRM call modify          0          0          0
                 entry !pre entry del  fsm failed fsm Succss
---------------- ---------- ---------- ---------- ----------
STRM call delete          0          0          0          0
---------------- ---------- ---------- ---------- ----------

             gccb !fnd entry !pre fsm failed fsm Succss
----------- ---------- ---------- ---------- ----------
call  stats          0          0          0          0
            fsm failed fsm Succss  entry del
----------- ---------- ---------- ---------- ----------
call  timer          0          0          0
            fsm failed fsm Succss
----------- ---------- ---------- ---------- ----------
stats timer          0          0
            entry !pre     rsp ok rsp failed
----------- ---------- ---------- ---------- ----------
provisn rsp          0          2          0
            fsm Succss fsm failed entry deld
----------- ---------- ---------- ---------- ----------
                     2          0          0
```

```
            entry !pre     rsp ok rsp failed fsm Succes
----------- ---------- ---------- ---------- ----------
 delete rsp          0          0          0          0
            fsm failed entry deld corr mismt inval gccb
----------- ---------- ---------- ---------- ----------
                     0          0          0          0
type        entry !pre     rsp ok rsp failed InvGCCB
----------- ---------- ---------- ---------- ----------
 stats  rsp          0          0          0          0
type        fsm Succss fsm failed corr mismt
----------- ---------- ---------- ---------- ----------
                     0          0          0
type       entry !pre mda DN App mda UP App srtp ROC upd lpbk mda DN lpbk mda UP Cor !match
 InvGCCB
----------- ---------- ---------- ---------- ------------ ----------- ----------- ----------
 ----------
 media evnt          0          0          2            1           0           0
 0          0

HA Stats

TDM-TDM Stats
            add sent T entry Fail entry insr fsm Succss
----------- ---------- ---------- ---------- ----------
tdm create          0          0          0          0
            fsm failed ent delete       fail
----------- ---------- ---------- ---------- ----------
                     0          0          0

            entry !pre fsm failed fsm Succss
----------- ---------- ---------- ---------- ----------
tdm modify          0          0          0
            entry !pre entry del  fsm failed fsm Succss
----------- ---------- ---------- ---------- ----------
tdm delete          0          0          0          0
            fsm failed fsm Succss  entry del
----------- ---------- ---------- ---------- ----------
 tdm  timer          0          0          0

            entry !pre     rsp ok rsp failed
----------- ---------- ---------- ---------- ----------
tdm prv rsp         0          0          0
            fsm Succss fsm failed entry deld
----------- ---------- ---------- ---------- ----------
                     0          0          0
            entry !pre     rsp ok rsp failed fsm Succes
----------- ---------- ---------- ---------- ----------
tdm del rsp         0          0          0          0
            fsm failed entry deld
----------- ---------- ----------
                     0          0

Single/Conferee Leg Stats
--------------- ---------- ---------- ---------- ----------
                gccb/rtpNL pr gccb NL no gccb sd badConfIds
--------------- ---------- ---------- ---------- ----------
singl/conf add           0          0          0          0
                add sent   entry Fail entry insr fsm Succss
--------------- ---------- ---------- ---------- ----------
singl/conf add          0          0          0          0
                fsm failed ent delete req_fail
--------------- ---------- ---------- ---------- ----------
singl/conf add          0          0          0
```

```
               entry !pre fsm failed fsm Succss
-------------- ---------- ---------- ---------- ----------
singl/conf mod          0          0          0
               entry !pre entry del  fsm failed fsm Succss
-----------  ---------- ---------- ---------- ----------
singl/conf del          0          0          0          0

********************** ACTIVE ******************************
               FORK_SESS_IDLE FORK_SESS_ALLOCATING FORK_SESS_ALLOCATED FORK_SESS_MODIFYING
FORK_SESS_CREATE_REQ               0                0                0                0
FORK_SESS_MODIFY_REQ               0                0                0                0
FORK_SESS_DELETE_REQ               0                0                0                0
FORK_SESS_GET_STATS_REQ               0                0                0                0
FORK_SESS_PROV_RSP_OK                0                0                0                0
FORK_SESS_PROV_RSP_FAIL               0                0                0                0
FORK_SESS_DELETE_RSP               0                0                0                0
FORK_SESS_GET_STATS_RSP               0                0                0                0
FORK_SESS_STATS_TMR_EXP               0                0                0                0
FORK_SESS_TMR_EXPIRY               0                0                0                0
               FORK_SESS_DELETING FORK_SESS_DELETE_PENDING
FORK_SESS_CREATE_REQ               0                0
FORK_SESS_MODIFY_REQ               0                0
FORK_SESS_DELETE_REQ               0                0
FORK_SESS_GET_STATS_REQ               0                0
FORK_SESS_PROV_RSP_OK                0                0
FORK_SESS_PROV_RSP_FAIL               0                0
FORK_SESS_DELETE_RSP               0                0
FORK_SESS_GET_STATS_RSP               0                0
FORK_SESS_STATS_TMR_EXP               0                0
FORK_SESS_TMR_EXPIRY               0                0
********************** END ACTIVE ****************************


********************** STANDBY *****************************
               FORK_SESS_IDLE FORK_SESS_ALLOCATING FORK_SESS_ALLOCATED FORK_SESS_MODIFYING
FORK_SESS_CREATE_REQ               0                0                0                0
FORK_SESS_MODIFY_REQ               0                0                0                0
FORK_SESS_DELETE_REQ               0                0                0                0
FORK_SESS_GET_STATS_REQ               0                0                0                0
FORK_SESS_PROV_RSP_OK                0                0                0                0
FORK_SESS_PROV_RSP_FAIL               0                0                0                0
FORK_SESS_DELETE_RSP               0                0                0                0
FORK_SESS_GET_STATS_RSP               0                0                0                0
FORK_SESS_STATS_TMR_EXP               0                0                0                0
FORK_SESS_TMR_EXPIRY               0                0                0                0
               FORK_SESS_DELETING FORK_SESS_DELETE_PENDING
FORK_SESS_CREATE_REQ               0                0
FORK_SESS_MODIFY_REQ               0                0
FORK_SESS_DELETE_REQ               0                0
FORK_SESS_GET_STATS_REQ               0                0
FORK_SESS_PROV_RSP_OK                0                0
FORK_SESS_PROV_RSP_FAIL               0                0
FORK_SESS_DELETE_RSP               0                0
FORK_SESS_GET_STATS_RSP               0                0
FORK_SESS_STATS_TMR_EXP               0                0
FORK_SESS_TMR_EXPIRY               0                0
********************** END STANDBY ***************************


Correlators in use:0

Corrupted table error (alloc):0
```

```
Corrupted table error (delete):0
----------- ---------- ---------- ---------- ----------
            gccb/rtpNL pr gccb NL no gccb sd badConfIds
----------- ---------- ---------- ---------- ----------
fork_sess create          0          0          0          0
            add sent T entry Fail entry insr fsm Succss
----------- ---------- ---------- ---------- ----------
                      0          0          0          0
            fsm failed ent delete       fail
----------- ---------- ---------- ---------- ----------
                      0          0          0

            entry !pre fsm failed fsm Succss
----------- ---------- ---------- ---------- ----------
Fork session modify          0          0          0
            entry !pre entry del  fsm failed fsm Succss
----------- ---------- ---------- ---------- ----------
fork_sess delete          0          0          0          0

---------------- ---------- ---------- ---------- ----------

             gccb !fnd entry !pre fsm failed fsm Succss
----------- ---------- ---------- ---------- ----------
fork_sess  stats          0          0          0          0
            fsm failed fsm Succss  entry del
----------- ---------- ---------- ---------- ----------
fork_sess  timer          0          0          0
            fsm failed fsm Succss
----------- ---------- ---------- ---------- ----------
stats timer          0          0
            entry !pre     rsp ok rsp failed
----------- ---------- ---------- ---------- ----------
provisn rsp          0          0          0
            fsm Succss fsm failed entry deld
----------- ---------- ---------- ---------- ----------
                      0          0          0
            entry !pre     rsp ok rsp failed fsm Succes
----------- ---------- ---------- ---------- ----------
 delete rsp          0          0          0          0
            fsm failed entry deld corr mismt inval gccb
----------- ---------- ---------- ---------- ----------
                      0          0          0          0
type        entry !pre     rsp ok rsp failed InvGCCB
----------- ---------- ---------- ---------- ----------
----------- ---------- ---------- ---------- ----------
 stats  rsp          0          0          0          0
type        fsm Succss fsm failed corr mismt
----------- ---------- ---------- ---------- ----------
                      0          0          0

media event rate:60 per 100msec, media timeout:50 secs
```

Cisco IOS XE Gibraltar 16.12.1a added information about SRTP Rollover Counter (ROC) in the command output. In the above sample output, **srtp ROC upd** represents the total number of ROC updates received from data plane to control plane.

show voip htsp

To display the voip and hybrid transport switching protocol (HTSP) connections active in the router, use the **show voip htsp**command in privileged EXEC mode.

show voip htsp info [**controller** [**T1** *slot-number*]]

Syntax Description

info	Displays htsp related information.
controller	(Optional) Displays information about controllers such as DS3,T1,and E1.
T1	(Optional) Displays information about T1 controller.
slot-number	(Optional) controller slot number.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
15.0(1)M	This command was introduced in a release earlier than Cisco IOS Release 15.0(1)M.

Usage Guidelines

Use the**show voip htsp command to**display the voip and hybrid transport switching protocol (HTSP) connections active in the router.

Examples

The following is sample output from the **show voip htsp** command:

```
Router# show voip htsp
NOTE: '-' means Not Applicable for that signalling type
  SLOT/                                                 TSP        TDM      TDM
 PORT/                                    TSP          BEAR     CONNECT   CROSS
 CHANNEL    HTSPINFO    VTSP_CDB         CDB          CHAN_T     DONE   CONNECT
=========  ==========  ==========  ==========  ==========  =======  =======
 02/00/01  0x677371E8  0x68905A48  0x67757AA4  0x677371E8     y        y
 02/00/02  0x67737780  0x00000000  0x00000000  0x00000000     n        n
 02/00/03  0x67737D18  0x68906548  0x67757584  0x67737D18     y        y
 02/00/04  0x677382B0  0x68904C88  0x677572F4  0x677382B0     y        y
 02/00/05  0x67738848  0x00000000  0x00000000  0x00000000     n        n
 02/00/06  0x67738DE0  0x00000000  0x00000000  0x00000000     n        n
 02/00/07  0x67739378  0x689054C8  0x67756B44  0x67739378     y        y
 02/00/08  0x67739910  0x68907888  0x677568B4  0x67739910     y        y
 02/00/09  0x67739EA8  0x00000000  0x00000000  0x00000000     n        n
 02/00/10  0x6773A440  0x00000000  0x00000000  0x00000000     n        n
 02/00/11  0x6773A9D8  0x68906D88  0x67756104  0x6773A9D8     y        y
 02/00/12  0x6773AF70  0x68908388  0x67755E74  0x6773AF70     y        y
 02/00/13  0x6773B508  0x00000000  0x00000000  0x00000000     n        n
 02/00/14  0x6773BAA0  0x00000000  0x00000000  0x00000000     n        n
 02/00/15  0x6773C038  0x689096C8  0x677556C4  0x6773C038     y        y
 02/00/17  0x6773C5D0  0x68909148  0x67755434  0x6773C5D0     y        y
 02/00/18  0x6773CB68  0x00000000  0x00000000  0x00000000     n        n
 02/00/19  0x6773D100  0x00000000  0x00000000  0x00000000     n        n
 02/00/20  0x6773D698  0x68905788  0x67754C84  0x6773D698     y        y
 02/00/21  0x6773DC30  0x68905D08  0x677549F4  0x6773DC30     y        y
```

```
02/00/22  0x6773E1C8  0x00000000  0x00000000  0x00000000     n        n
02/00/23  0x6773E760  0x00000000  0x00000000  0x00000000     n        n
02/00/24  0x6773ECF8  0x68906AC8  0x67754244  0x6773ECF8     y        y
02/00/25  0x6773F290  0x68907308  0x67753FB4  0x6773F290     y        y
02/00/26  0x6773F828  0x00000000  0x00000000  0x00000000     n        n
02/00/27  0x6773FDC0  0x00000000  0x00000000  0x00000000     n        n
02/00/28  0x67740358  0x689080C8  0x67753804  0x67740358     y        y
02/00/29  0x677408F0  0x68908908  0x67753574  0x677408F0     y        y
02/00/30  0x67740E88  0x00000000  0x00000000  0x00000000     n        n
02/00/31  0x67741420  0x68909408  0x67753054  0x67741420     y        y
02/02/01  0x67B88824  0x00000000  0x00000000      -         -        n
02/02/02  0x67B88DBC  0x00000000  0x00000000      -         -        n
02/02/03  0x67B89354  0x00000000  0x00000000      -         -        n
02/02/04  0x67B898EC  0x00000000  0x00000000      -         -        n
02/02/05  0x67B89E84  0x00000000  0x00000000      -         -        n
02/02/06  0x67B8A41C  0x00000000  0x00000000      -         -        n
02/02/07  0x67B8A9B4  0x00000000  0x00000000      -         -        n
02/02/08  0x67B8AF4C  0x00000000  0x00000000      -         -        n
02/02/09  0x67B8B4E4  0x00000000  0x00000000      -         -        n
```

Related Commands

Command	Description
debug voip vtsp	Displays information about the voice telephony service provider (VTSP).

show voip recmsp session

To display active recording Media Service Provider (MSP) session information, use the **show voip recmsp session** command in privileged EXEC mode.

show voip recmsp session [**detail**] { **call-id** *call-id* | **forked call-id** *call-id* }

Syntax Description

detail	(Optional) Displays detailed active session information.
forked	Displays forked session information.
call-id *callid*	(Optional) Specifies the recording MSP call ID. The range is from 1 to 2147483647.

Command Default

Displays brief information about recorded calls that have the anchor call ID, forked call ID, and MSP call ID.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
15.2(1)T	This command was introduced.
Cisco IOS XE 17.18.1a	The **forked call-id** *call-id* parameter is added to support display of forked and associated anchored session information.

Usage Guidelines

Use the **show voip recmsp session** command to display MSP-related information about the recorder, for example, the way the recording MSP views the recording session.

The **show voip recmsp session detail call-id** *callid* command provides detailed information about each recording session. It provides details about the anchor leg and nonanchor leg. It also shows how the anchor and nonanchor streams are mapped to the forked leg Real-Time Transport Protocol (RTP) streams.

The **show voip recmsp session detail forked call-id** *callid* command provides detailed forked session information.

Examples

The following is a sample output from the **show voip recmsp session detail call-id** command. Fields in the display are self-explanatory.

```
Device# show voip recmsp session detail call-id 140

RECMSP active sessions:
Detailed Information
========================
Recording MSP Leg Details:
Call ID: 143
GUID : 7C5946D38ECD
AnchorLeg Details:
Call ID: 141
Forking Stream type: voice-nearend
Participant: 708090
Non-anchor Leg Details:
```

```
Call ID: 140
Forking Stream type: voice-farend
Participant: 10000
Forked Leg Details:
Call ID: 145
Voice Near End Stream CallID 145
Stream State ACTIVE
Voice Far End stream CallID 146
Stream State ACTIVE
Found 1 active sessions
```

The following is a sample output from the **show voip recmsp session** command:

```
Device# show voip recmsp session
RECMSP active sessions:
MSP Call-ID              AnchorLeg Call-ID        ForkedLeg Call-ID
13                       12                       14
Found 1 active sessions
```

The following is a sample output from the **show voip recmsp session detail forked call-id** *call-id* command:

```
Device# show voip recmsp session detail forked call-id 14
CC Call-ID: 12 Anchor:
 Dur: 00:00:13 Dialpeer-Tag: 9:
  Stream 1: voice-only
   tx: 1391/278200 rx: 891/178200
   Remote-Addr: 10.10.10.162:6000, Local-Addr: 10.10.10.195:8018
   Status: ACTIVE

CC Call-ID: 14 Forked:
 Dur: 00:00:13 Dialpeer-Tag: 10:
  Stream 1: voice-nearend
   tx: 1391/278200
   Remote-Addr: 10.10.10.162:6000, Local-Addr: 10.10.10.195:8020
   Status: ACTIVE
  Stream 2: voice-farend
   tx: 891/178200
   Remote-Addr: 10.10.10.162:6002, Local-Addr: 10.10.10.195:8022
   Status: ACTIVE
Found 1 active sessions
```

Related Commands

Command	Description
media-recording	Configures voice class recording parameters.

show voip rtp connections

To display Real-Time Transport Protocol (RTP) named event packets, use the **show voip rtp connections** command in privileged EXEC mode.

show voip rtp connections [**detail**]

Syntax Description

detail	(Optional) Displays the called-party and calling-party numbers associated with a call.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.0	This command was introduced.
12.3(7)T	The **detail** keyword was added.
12.3(14)T	This command was implemented on the Cisco 2800 series and Cisco 3800 series.
12.4(2)T	This command was integrated into Cisco IOS Release 12.4(2)T.
12.4(22)T	Command output was updated to show IPv6 information.
Cisco IOS 15.6(2)T	The command output was enhanced to show VRF information.
Cisco IOS XE Gibraltar 16.12.1a	The command output was enhanced to show SRTP Rollover Counter (ROC) information.
Cisco IOS XE Gibraltar 16.12.2	The command output was updated to show SRTP Rollover Count (ROC) information based on Remote IP address and Port.

Usage Guidelines

This command displays information about RTP named event packets, such as caller ID number, IP address, and port for both the local and remote endpoints. The output from this command provides an overview of all the connections in the system, and this information can be used to narrow the criteria for debugging. The **debug voip rtp** command floods the console with voice packet information. You can use the **show voip rtp connections** command to get caller ID, remote IP address, or remote port identifiers that you can use to limit the output from the **debug voip rtp** command.

The **detail** keyword allows you to identify the phone or phones that have connected two RTP call legs to create VoIP-to-VoIP or VoIP-to-POTS hairpins. If the **detail** keyword is omitted, the output does not display calls that are connected by hairpin call routing.

Examples

The table below describes the significant fields shown in the examples. Each line of output under "VoIP RTP active connections" shows information for one call leg. A phone call normally consists of two call legs, one connected to the calling party and one connected to the called party. The router joins (or bridges) the two call legs to make a call. The **show voip rtp connections** command shows the RTP information for H.323 and Session Initiation Protocol (SIP) calls only; it does not directly

show the POTS call legs. The information for the IP phone can be seen using the **show ephone offhook** command.

The following sample output shows an incoming H.323 call that is being directed to an IP phone attached to a Cisco Unified Communications Manager Express (Unified CME) system.

```
Router# show voip rtp connections
VoIP RTP active connections :
No. CallId  dstCallId  LocalRTP RmtRTP LocalIP          RemoteIP
1   21      22         16996    18174  10.4.204.37      10.4.204.24
Found 1 active RTP connections
```

The following sample output shows the same call as in the previous example, but using the **detail** keyword with the command. The sample output shows the called number (1509) and calling number (8108) on both call legs (21 and 22); the called and calling numbers are the same on both legs for a simple A-to-B call. Leg 21 is the H.323 segment of the and leg 22 is the POTS segment that goes to the IP phone.

```
Router#
show voip rtp connections detail
VoIP RTP active connections :
No. CallId  dstCallId  LocalRTP RmtRTP LocalIP          RemoteIP
1   21      22         16996    18174  10.4.204.37      10.4.204.24
  callId 21 (dir=1):called=1509 calling=8108 redirect=
     dest callId 22:called=1509 calling=8108 redirect=
   1 context 64FB3358 xmitFunc 6032E8B4
Found 1 active RTP connections
```

The following example shows the call from the previous example being transferred by extension 1509 to extension 1514. Notice that the dstCallId changed from 22 to 24, but the original call leg (21) for the transferred party is still present. This implies that H.450.2 capability was disabled for this particular call, because if H.450.2 was being used for the transfer, the transfer would have caused the incoming H.323 call leg to be replaced with a new call.

```
Router# show voip rtp connections

VoIP RTP active connections :
No. CallId  dstCallId  LocalRTP RmtRTP LocalIP         RemoteIP
1   21      24         16996    18174  10.4.204.37      10.4.204.24
Found 1 active RTP connections
```

The following example shows the detailed output for the same transfer as shown in the previous example. The original incoming call leg is still present (21) and still has the original called and calling numbers. The transferred call leg (24) shows 1509 (the transferring party) as the calling party and 1514 (the transfer destination) as the called party.

```
Router# show voip rtp connections detail
VoIP RTP active connections :
No. CallId  dstCallId  LocalRTP RmtRTP LocalIP         RemoteIP
1   21      24         16996    18174  10.4.204.37      10.4.204.24
  callId 21 (dir=1):called=1509 calling=8108 redirect=
     dest callId 24:called=1514 calling=1509 redirect=
   1 context 6466E810 xmitFunc 6032E8B4
Found 1 active RTP connections
```

The following sample output shows a cross-linked call with two H.323 call legs. The first line of output shows that the CallID for the first call leg is 7 and that this call leg is associated with another call leg that has a destination CallId of 8. The next line shows that the CallID for the leg is 8 and that

it is associated with another call leg that has a destination CallId of 7. This cross-linkage between CallIds 7 and 8 shows that the first call leg is related to the second call leg (and vice versa). From this you can infer that the two call legs are actually part of the same phone call.

In an active system you can expect many lines of output that you would have to sort through to see which ones have this cross-linkage relationship. The lines showing two related call legs are not necessarily listed in adjacent order.

```
Router# show voip rtp connections
VoIP RTP active connections :
No. CallId   dstCallId          LocalRTP     RmtRTP         LocalIP         RemoteIP
1        7           8             16586      22346      172.27.82.2      172.29.82.2
2        8           7             17010      16590      172.27.82.2      192.168.1.29

Found 2 active RTP connections
```

The following example shows RTP information with IPv6 local and remote addresses:

```
Router# show voip rtp connections
VoIP RTP active connections :
No.  CallId   dstCallId  LocalRTP  RmtRTP   LocalIP                                RemoteIP
1     11      9          17424     18282    2001:DB8:C18:1:218:FEFF:FE71:2AB6
2001:DB8:C18:1:218:FEFF:FE71:2AB6
2     12      10         18282     17424    2001:DB8:C18:1:218:FEFF:FE71:2AB6
2001:DB8:C18:1:218:FEFF:FE71:2AB6
Found 2 active RTP connections
```

The following example shows RTP information with VRF details:

```
Router# show voip rtp connections
VoIP RTP Port Usage Information:
Max Ports Available: 23001, Ports Reserved: 101, Ports in Use: 2
Min Max Ports Ports Ports
Media-Address Range Port Port Available Reserved In-use
------------------------------------------------------------------------------
Global Media Pool 8000 48198 19999 101 2
------------------------------------------------------------------------------
VoIP RTP active connections :
No.   CallId  dstCallId    LocalRTP    RmtRTP     LocalIP     RemoteIP   MPSS    VRF
1      1        2           25000     16390    10.0.0.1     10.0.0.2     NO     VRF1
2      2        1           25002     16398    11.0.0.1     11.0.0.2     NO     VRF2
```

SRTP Rollover Counter (ROC) information is displayed in the “SSRC:ROC” format and is updated based on Remote IP address and Port.

The following example shows SRTP ROC information for an SRTP call:

```
Router#show voip rtp connections detail
VoIP RTP Port Usage Information:
Max Ports Available: 59794, Ports Reserved: 206, Ports in Use: 2
Port range configured
                                      Min   Max   Ports     Ports     Ports
Media-Address Range                   Port  Port  Available Reserved  In-use
------------------------------------------------------------------------------
Global Media Pool                     5500  65498 29897     103       2

IP Address Based Media Pool
------------------------------------------------------------------------------
8.39.15.21          8.39.15.21        5500  65498 29897     103       0
        Port-Range                    10000 20000
------------------------------------------------------------------------------
```

```
VoIP RTP active connections :
No. CallId     dstCallId  LocalRTP RmtRTP   LocalIP
RemoteIP                                  MPSS  VRF
1     323        324        5508     9256     10.64.86.90
10.65.105.60                              NO    NA
 callId 323 (dir=1): called=6010 calling=7776 redirect= loopback=NO confID=3 mode=3
rtp(tx:0/rx:0) rtcp(tx:0/rx:0) MPSS NO VRF NA                 peer callId 324: called=6010
 calling=7776 redirect= , confID:3
 , vrf = NA
   1 context 0x7F8FD8A428D0 xmitFunc 0x5605693121F0
2     324        323        5510     31826    10.64.86.90
10.64.88.52                               NO    NA
 callId 324 (dir=2): called=6010 calling=7776 redirect= loopback=NO confID=3 mode=3
rtp(tx:0/rx:0) rtcp(tx:0/rx:0) MPSS NO VRF NA                 peer callId 323: called=6010
 calling=7776 redirect= , confID:3
 , vrf = NA
   1 context 0x7F8FD8B11698 xmitFunc 0x5605693121F0
SRTP information for endpoints:
============================================================
remote ip = 10.64.88.52, remote port=31826
 RX SRTP ROC Context (SSRC:ROC): 0xBF85C508:0x1
 TX SRTP ROC Context (SSRC:ROC): 0x1E4E1915:0x1
------------------------------------------------------------
Found 2 active RTP connections
```

In the above example, **0xBF85C508** is the Synchronization Source (SSRC) and **0x1** is the ROC. **RX SRTP ROC Context** is the crypto SRTP context for all the received streams for a media session. **TX SRTP ROC Context** is the crypto SRTP context for all the transmitted streams for a media session.

ROC increases after every RTP sequence number (maximum of 65535) roll over.

```
Router#show voip rtp connections detail
VoIP RTP Port Usage Information:
Max Ports Available: 59794, Ports Reserved: 206, Ports in Use: 2
Port range configured
                                       Min   Max   Ports     Ports     Ports
Media-Address Range                    Port  Port  Available Reserved  In-use
-------------------------------------------------------------------------------
Global Media Pool                      5500  65498 29897     103       2

IP Address Based Media Pool
-------------------------------------------------------------------------------
8.39.15.21          8.39.15.21         5500  65498 29897     103       0
        Port-Range                     10000 20000
-------------------------------------------------------------------------------
VoIP RTP active connections :
No. CallId     dstCallId  LocalRTP RmtRTP   LocalIP
RemoteIP                                  MPSS  VRF
1     323        324        5508     9256     10.64.86.90
10.65.105.60                              NO    NA
 callId 323 (dir=1): called=6010 calling=7776 redirect= loopback=NO confID=3 mode=3
rtp(tx:0/rx:0) rtcp(tx:0/rx:0) MPSS NO VRF NA                 peer callId 324: called=6010
 calling=7776 redirect= , confID:3
 , vrf = NA
   1 context 0x7F8FD8A428D0 xmitFunc 0x5605693121F0
2     324        323        5510     31826    10.64.86.90
10.64.88.52                               NO    NA
 callId 324 (dir=2): called=6010 calling=7776 redirect= loopback=NO confID=3 mode=3
rtp(tx:0/rx:0) rtcp(tx:0/rx:0) MPSS NO VRF NA                 peer callId 323: called=6010
 calling=7776 redirect= , confID:3
 , vrf = NA
   1 context 0x7F8FD8B11698 xmitFunc 0x5605693121F0
SRTP information for endpoints:
```

```
==========================================================
remote ip = 10.64.88.52, remote port=31826
 RX SRTP ROC Context (SSRC:ROC): 0xBF85C508:0x2
 TX SRTP ROC Context (SSRC:ROC): 0x1E4E1915:0x2
----------------------------------------------------------
Found 2 active RTP connections
```

In the above example, **0xBF85C508** is the Synchronization Source (SSRC) and **0x2** is the ROC.

```
Router#show voip rtp connections detail
VoIP RTP Port Usage Information:
Max Ports Available: 59794, Ports Reserved: 206, Ports in Use: 2
Port range configured
                                       Min   Max   Ports     Ports     Ports
Media-Address Range                    Port  Port  Available Reserved  In-use
-------------------------------------------------------------------------------
Global Media Pool                      5500  65498 29897     103       2

IP Address Based Media Pool
-------------------------------------------------------------------------------
8.39.15.21          8.39.15.21         5500  65498 29897     103       0
        Port-Range                     10000 20000
-------------------------------------------------------------------------------
VoIP RTP active connections :
No. CallId     dstCallId  LocalRTP RmtRTP   LocalIP
RemoteIP                                  MPSS  VRF
1     323        324        5508     9256     10.64.86.90
10.65.105.60                              NO    NA
 callId 323 (dir=1): called=6010 calling=7776 redirect= loopback=NO confID=3 mode=3
rtp(tx:0/rx:0) rtcp(tx:0/rx:0) MPSS NO VRF NA                 peer callId 324: called=6010
 calling=7776 redirect= , confID:3
 , vrf = NA
   1 context 0x7F8FD8A428D0 xmitFunc 0x5605693121F0
2     324        323        5510     31826    10.64.86.90
10.64.88.52                               NO    NA
 callId 324 (dir=2): called=6010 calling=7776 redirect= loopback=NO confID=3 mode=3
rtp(tx:0/rx:0) rtcp(tx:0/rx:0) MPSS NO VRF NA                 peer callId 323: called=6010
 calling=7776 redirect= , confID:3
 , vrf = NA
   1 context 0x7F8FD8B11698 xmitFunc 0x5605693121F0
SRTP information for endpoints:
==========================================================
remote ip = 10.64.88.52, remote port=31826
 RX SRTP ROC Context (SSRC:ROC): 0xBF85C508:0x1 0xF487C8FF:0x1 0xE127C8FF:0x1 0xC987C8FF:0x1
 0xD567C8FF:0x1
 TX SRTP ROC Context (SSRC:ROC): 0x1E4E1915:0x1 0xF487C8FF:0x1 0xE127C8FF:0x1 0xC987C8FF:0x1
 0xD567C8FF:0x1
----------------------------------------------------------
Found 2 active RTP connections
```

The above example shows ROC context on per SSRC basis when there are multiple SSRCs involved in a single media session (for example, during a video call).

In a High Availability scenario, the ROC updates are checkpointed and preserved across switchovers. An active router lists all the SSRCs that have received the ROC updates in the reverse chronological order. In the below example, **0xE502F046:0x2** has received ROC update most recently and **0x94A522FC:0x1** has received ROC update prior to it, and so on. If there are more than 5 SSRCs, then only the first five SSRCs (those which have received the ROC updates most recently) are considered for checkpointing.

The following example shows output from active router:

```
Device#show voip rtp connections detail
VoIP RTP Port Usage Information:
```

```
Max Ports Available: 59794, Ports Reserved: 206, Ports in Use: 2
Port range configured
                                        Min   Max   Ports     Ports     Ports
Media-Address Range                     Port  Port  Available Reserved  In-use
-------------------------------------------------------------------------------
Global Media Pool                       5500  65498 29897     103       2

IP Address Based Media Pool
-------------------------------------------------------------------------------
8.39.15.21          8.39.15.21          5500  65498 29897     103       0
       Port-Range                       10000 20000
-------------------------------------------------------------------------------
VoIP RTP active connections :
No. CallId     dstCallId  LocalRTP RmtRTP   LocalIP                              RemoteIP
                                  MPSS  VRF
1     3          4          5500     29330    10.64.86.90
10.64.88.11                              NO    NA
 callId 3 (dir=0): called=6010 calling=7010 redirect= loopback=NO confID=1 mode=3
rtp(tx:0/rx:0) rtcp(tx:0/rx:0) MPSS NO VRF NA                  peer callId 4: called=6010
 calling=7010 redirect= , confID:1
 , vrf = NA
   1 context 0x7F378AC01E38 xmitFunc 0x55CD6A2182C0
2     4          3          5502     17580    10.64.86.90
10.64.88.52                              NO    NA
 callId 4 (dir=0): called=6010 calling=7010 redirect= loopback=NO confID=1 mode=3
rtp(tx:0/rx:0) rtcp(tx:0/rx:0) MPSS NO VRF NA                  peer callId 3: called=6010
 calling=7010 redirect= , confID:1
 , vrf = NA
   1 context 0x7F37D1CE7A38 xmitFunc 0x55CD6A2182C0
SRTP information for endpoints:
============================================================
remote ip = 10.64.88.52, remote port=17580
 RX SRTP ROC Context (SSRC:ROC): 0xE502F046:0x2 0x94A522FC:0x1 0x79C19EC:0x1 0x8453A05E:0x8
 0xE27329A2:0x1 0xE08E9236:0x4 0xD8A97DA8:0x1 0xDCD0D1C7:0x1
 TX SRTP ROC Context (SSRC:ROC): 0xD22D83EE:0x2 0x8C9EFB1C:0x1 0x90A2D00C:0x1 0xD9C0D844:0x8
 0x54F9FA7D:0x1 0xDCA9E096:0x4 0x6D539A3B:0x1 0x5067FDE8:0x1
------------------------------------------------------------
Found 2 active RTP connections
```

The following example shows output from standby router:

```
Device#show voip rtp connections detail
VoIP RTP Port Usage Information:
Max Ports Available: 59794, Ports Reserved: 206, Ports in Use: 2
Port range configured
                                        Min   Max   Ports     Ports     Ports
Media-Address Range                     Port  Port  Available Reserved  In-use
-------------------------------------------------------------------------------
Global Media Pool                       5500  65498 29897     103       2

IP Address Based Media Pool
-------------------------------------------------------------------------------
8.39.15.21          8.39.15.21          5500  65498 29897     103       0
       Port-Range                       10000 20000
-------------------------------------------------------------------------------
VoIP RTP active connections :
No. CallId     dstCallId  LocalRTP RmtRTP   LocalIP                              RemoteIP
                                  MPSS  VRF
1     3          4          5500     29330    10.64.86.90
10.64.88.11                              NO    NA
 callId 3 (dir=0): called=6010 calling=7010 redirect= loopback=NO confID=1 mode=3
rtp(tx:0/rx:0) rtcp(tx:0/rx:0) MPSS NO VRF NA                  peer callId 4: called=6010
 calling=7010 redirect= , confID:1
 , vrf = NA
2     4          3          5502     17580    10.64.86.90
```

```
10.64.88.52                                  NO    NA
 callId 4 (dir=0): called=6010 calling=7010 redirect= loopback=NO confID=1 mode=3
rtp(tx:0/rx:0) rtcp(tx:0/rx:0) MPSS NO VRF NA                  peer callId 3: called=6010
 calling=7010 redirect= , confID:1
 , vrf = NA
SRTP information for endpoints:
=========================================================
remote ip = 10.64.88.52, remote port=17580
 RX SRTP ROC Context (SSRC:ROC): 0xE502F046:0x2 0x94A522FC:0x1 0x79C19EC:0x1 0x8453A05E:0x8
 0xE27329A2:0x1
 TX SRTP ROC Context (SSRC:ROC): 0xD22D83EE:0x2 0x8C9EFB1C:0x1 0x90A2D00C:0x1 0xD9C0D844:0x8
 0x54F9FA7D:0x1
---------------------------------------------------------
Found 2 active RTP connections
```

Table 205: show voip rtp connections Field Descriptions

Field	Description
No.	Identifier of an RTP connection in this output.
CallId	Internal call identifier of a telephony call leg (RTP connection).
dstCallId	Internal call identifier of a VoIP call leg.
LocalRTP	RTP port of the media stream for the local entity.
RmtRTP	RTP port of the media stream for the remote entity.
LocalIP	IPv4 or IPv6 address of the media stream for the local entity.
RemoteIP	IPv4 or IPv6 address of the media stream for the remote entity.
dir	0 indicates an outgoing call. 1 indicates an incoming call.
called	Extension that received the call.
calling	Extension that made the call.
redirect	Original called number if the incoming call was forwarded.
context	Internal memory address for the control block associated with the call.
xmitFunc	Internal memory address for the transmit function to which incoming RTP packets (on the H.323 and SIP side) are sent; the address for the function that delivers the packets to the ephone.
VRF	Virtual Routing and Forwarding (VRF) associated with the call.
SSRC:Index	SRTP Rollover Counter information.
RX SRTP ROC Context	The crypto SRTP context for all the received streams for a media session.
TX SRTP ROC Context	The crypto SRTP context for all the transmitted streams for a media session.

Related Commands

Command	Description
debug voip rtp	Enables debugging for RTP named event packets.
show ephone offhook	Displays information and packet counts for phones that are currently off hook.

show voip rtp forking

To display the Real-Time Transport Protocol (RTP) media-forking connections, use the **show voip rtp forking** command in privileged EXEC mode.

show voip rtp forking

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.4(24)T	This command was introduced in a release earlier than Cisco IOS Release 12.4(24)T.

Usage Guidelines

The **show voip rtp forking** command displays information about RTP named event packets, such as type of stream, IP address, and port for both the local and remote endpoints. The output from this command provides an overview of all the media-forking connections in the system, and this information can be used to narrow the criteria for debugging. The **debug voip rtp** command floods the console with voice packet information. You can use the **show voip rtp forking** command to display the remote IP address, or remote port identifiers that you can use to limit the output from the **debug voip rtp** command.

Examples

The following is sample output from the **show voip rtp forking** command:

```
Router# show voip rtp forking
VoIP RTP active forks :
 Fork 1
   stream type voice-only (0): count 1
     remote ip 9.13.36.101,  remote port 20590,  local port 17596
       codec g711alaw,  logical ssrc 0x60
       packets sent 237,  packets received 413
   stream type voice+dtmf (1): count 0
   stream type dtmf-only (2): count 0
   stream type voice-nearend (3): count 1
     remote ip 9.13.36.102,  remote port 18226,  local port 17434
       codec g729r8,  logical ssrc 0x103
       packets sent 39,  packets received 0
   stream type voice+dtmf-nearend (4): count 0
   stream type voice-farend (5): count 1
     remote ip 9.13.36.120,  remote port 16912,  local port 21098
       codec g729r8,  logical ssrc 0x105
       packets sent 39,  packets received 0
   stream type voice+dtmf-farend (6): count 0
   stream type video (7): count 0
```

The table below describes the significant fields shown in the display.

Table 206: show voip rtp forking Field Descriptions

Field	Description
stream type	Indicates the type of stream.

Field	Description
count	Number of packets in the specified type of stream.
remote ip	IPv4 or IPv6 address of the media stream for the remote entity.
remote port	RTP port of the media stream for the remote entity.
local port	RTP port of the media stream for the local entity.
codec	Codec supported on the specified channel.
logical ssrc	Indicates the logical synchronization source (SSRC) for the specified channel.
packets sent	Total number of packets sent from the channel.
packets received	Total number of packets received by the channel.

Related Commands

Command	Description
debug voip rtp	Enables debugging for RTP named event packets.

show voip rtp stats

To display the RTP statistics and error counters based on the configuration.

show voip rtp stats

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Release 3.9S	This command was introduced.
Cisco IOS XE Bengaluru 17.4.1a	Earlier, 'show voip rtp stats' command displayed details of ports that are allocated from the global port table only. From Cisco IOS XE Bengaluru 17.4.1a onwards, this command also displays details of ports that are allocated from the following port tables: • Media IP address based tables • Media VRF-based tables A unique identifier is generated and displayed for each table, which serves as a reference to 'clear voip rtp port' command.

The following examples display port allocations from multiple tables:

```
Router# show voip rtp stats
------------
RTP DP stats
------------
 DP:     add     add-pend   add-video     mod     mod-!rtp   del-leg1  del/dstroy
---- ---------- ---------- ---------- ---------- ---------- ---------- ----------
              4          0          0          0          0          0          0
 DP LPBK:    add     add-video     mod     mod-!rtp    del-leg1  del/dstroy
--------- ---------- ---------- ---------- ---------- ---------- ----------
                    0          0          0          0          0          0
 DP single leg:    add     mod     del/dstroy
---------------    -----   -----   -----------
                   0          0          0
 DP conf leg  :    add     mod     del/dstroy
---------------    -----   -----   -----------
                   0          0          0

dp_mod_dst_zero                 :          16
dp_mod_no_change                :          32
dp_skip_mod_addnotdone          :           8


 VOIP RTP Max Media Loop Count : 6

VOIP RTP Stats Counters :
GCCB:Inserted =8        Removed =0
PORT:Allocated=8        Reserved=0        Released=0        Invalid Index=0        Port
Overwrite=0
```

```
SIPSPI:Leak(Avoided=0        Suspected=0       ) Lost Port Handle=0
RTSP:Leak(Avoided=0        Suspected=0       )

 VOIP RTP Error Counters :
        gccb null invalid callid (6) count  = 8
        gccb null for callid (7) count  = 18

 2 errortypes observed

                                        Min   Max   Ports     Ports     Ports
Media-Address Range                     Port  Port  Available Reserved  In-use
-------------------------------------------------------------------------------
Global Media Pool (ID :1)               10000 40000 14900     101       0

Port   GCCB Status  CallID   Src Port   Leak?  No call
-------------------------------------------------------

                                        Min   Max   Ports     Ports     Ports
IP Address Based Media Pool (ID :4)     Port  Port  Available Reserved  In-use
-------------------------------------------------------------------------------------------
8.43.21.94          8.43.21.94          20000 30000 4900      101       4

Port   GCCB Status  CallID   Src Port   Leak?  No call
-------------------------------------------------------
20000  Inserted     1        20000      N      N
20002  Inserted     4        20002      N      N
20004  Inserted     5        20004      N      N
20006  Inserted     8        20006      N      N

                                        Min   Max   Ports     Ports     Ports
IP Address Based Media Pool (ID :5)     Port  Port  Available Reserved  In-use
-------------------------------------------------------------------------------------------
10.65.125.167       10.65.125.167       25000 35000 5001      0         0

Port   GCCB Status  CallID   Src Port   Leak?  No call
-------------------------------------------------------

                                        Min   Max   Ports     Ports     Ports
IP Address Based Media Pool (ID :6)     Port  Port  Available Reserved  In-use
-------------------------------------------------------------------------------------------
2001:DB8:85A3::8A2E:370:7334
2001:DB8:85A3::8A2E:370:8800            20000 30000 4900      101       0

Port   GCCB Status  CallID   Src Port   Leak?  No call
-------------------------------------------------------

                                        Min   Max   Ports     Ports     Ports
VRF ID Based Media Pool (ID :2)         Port  Port  Available Reserved  In-use
-------------------------------------------------------------------------------------------
VRF1                                    14000 48000 16900     101       2

Port   GCCB Status  CallID   Src Port   Leak?  No call
-------------------------------------------------------
14000  Inserted     6        14000      N      N
14002  Inserted     7        14002      N      N

                                        Min   Max   Ports     Ports     Ports
VRF ID Based Media Pool (ID :3)         Port  Port  Available Reserved  In-use
-------------------------------------------------------------------------------------------
VRF2                                    20000 48000 13900     101       2

Port   GCCB Status  CallID   Src Port   Leak?  No call
-------------------------------------------------------
20000  Inserted     2        20000      N      N
```

```
20002  Inserted     3        20002      N      N

Total=513, GCCB(Inserted=8, Deleted=0, Null=0 Possible Leaked=0, Blocked=505)
-------------------------------------------------------------------------------
```

The following example displays hung ports in a call scenario. There are two ways to determine the hung ports:

- Check the "Possible Leaked" value in the **show voip rtp stats** command output. The "Possible Leaked" value gives the total number of hung ports in all the port tables.
- Check the "Leak" flag value in each table. If it is "Y", then it is a hung port.

```
Router# show voip rtp stats
                                        Min   Max   Ports     Ports     Ports
Media-Address Range                     Port  Port  Available Reserved  In-use
-------------------------------------------------------------------------------
Global Media Pool (ID :1)               8000  48198 19999     101       0

Port   GCCB Status  CallID   Src Port   Leak?  No call
-------------------------------------------------------------

                                        Min   Max   Ports     Ports     Ports
IP Address Based Media Pool (ID :2)     Port  Port  Available Reserved  In-use
-------------------------------------------------------------------------------------------------
8.43.21.94          8.43.21.94          10000 40000 14900     101       3

Port   GCCB Status  CallID   Src Port   Leak?  No call
-------------------------------------------------------------
10024    Null                           Y
10028    Null                           Y
10034    Null                           Y

Total=205, GCCB(Inserted=0, Deleted=0, Null=3, Possible Leaked=3, Blocked=202)
-------------------------------------------------------------------------------


CSR#clear voip rtp port 2 10024,10028,10034
Any port(s) associated with an active call will not be cleared.[confirm]
Cleared port 10024
Cleared port 10028
Cleared port 10034
```

show voip rtp stats command after releasing hung ports. You can determine that there are no hung ports by performing the following:

- Check the "Possible Leaked" value in the **show voip rtp stats** command output. The "Possible Leaked" value should be zero.
- Check the "Leak" flag value in each port table. The values are removed from the tables.

```
                                        Min   Max   Ports     Ports     Ports
Media-Address Range                     Port  Port  Available Reserved  In-use
-------------------------------------------------------------------------------
Global Media Pool (ID :1)               8000  48198 19999     101       0

Port   GCCB Status  CallID   Src Port   Leak?  No call
-------------------------------------------------------------
```

```
                                        Min   Max   Ports     Ports     Ports
IP Address Based Media Pool (ID :2)     Port  Port  Available Reserved  In-use
-------------------------------------------------------------------------------------------
8.43.21.94          8.43.21.94          10000 40000 14900     101       0

Port   GCCB Status  CallID   Src Port   Leak?  No call
-------------------------------------------------------------

Total=202, GCCB(Inserted=0, Deleted=0, Null=0, Possible Leaked=0, Blocked=202)
-------------------------------------------------------------------------------
```

show voip stream-service callid

To display detailed information about a WebSocket call using the call ID that initiated the media forking request, use the **show voip stream-service callid** *callid* command in privileged EXEC mode.

show voip stream-service callid *callid*

Syntax Description

callid	The call control call-ID of a WebSocket call that initiated the media forking request.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Bengaluru 17.6.1a	This command was introduced.

Usage Guidelines

The following are some of the details about the WebSocket call displayed by this show command:

- WebSocket ID
- Fork Session ID
- Call GUID
- Near-end Channel ID
- Far-end Channel ID
- Status
- TX/RX packets replicated
- TX/RX octets replicated
- TX/RX packets dropped
- TX/RX octets dropped

Examples

The following is a sample output for the command **show voip stream-service callid** *callid* for a call ID associated with a WebSocket connection.

```
router#Show voip stream-service callid 18
WebSocket id          : 11
Fork session id       : 2
Call GUID             : 3FBF760000010000001FF2691D0816AC
Near-end channel id   : 3
Far-end channel id    : 4
Status                : Active

TX packets replicated : 231
TX octets replicated  : 36960
TX packets dropped    : 0
TX octets dropped     : 0
RX packets replicated : 231
```

```
RX octets replicated  : 36960
RX packets dropped    : 0
RX octets dropped     : 0
```

The table describes significant fields shown in this output.

Table 207: Show voip stream-service callid <callid> Field Descriptions

WebSocket ID	The unique ID number associated with a WebSocket connection.
Fork Session ID	The ID number associated with the fork session of a WebSocket connection.
Call GUID	The unique ID for a WebSocket call.
Near-end Channel ID	The unique ID for the near-end (CVP side) channel of the forked call.
Far-end Channel ID	The unique ID for the far-end (CUBE side) channel of the forked call.
Status	The status of WebSocket forking: Active (media forking is in progress), Paused (media forking is on hold), Stopped (media forking is stopped).

Related Commands

Command	Description
show voip stream-service connection	Displays information about the active WebSocket connections in Unified Border Element.
show voip stream-service connection history	Displays information about all the closed WebSocket connections in Unified Border Element.
show voip stream-service server <ip:port>	Displays information about the WebSocket connection based on WebSocket server IP and port.

show voip stream-service connection

To display information about all the active WebSocket connections in CUBE, use the **show voip stream-service connection** command in privileged EXEC mode.

show voip stream-service connection

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Bengaluru 17.6.1a	This command was introduced.

Usage Guidelines

Use this command to display the list of WebSocket connections in active state. The number of active calls and total calls is displayed for each of the active WebSocket connections. **Active Calls** are the count of active calls that uses this WebSocket connection for forking. **Total Calls** are the total number of calls that used this WebSocket connection for forking.

CUBE displays information on the **Remote Hostname** and port instead of remote IP address and port in the following scenarios:

- The JSON encoded MIME attachment in the SIP re-INVITE contains remote hostname instead of remote IP address.
- The CLI command **proxy** is configured under media profile configuration mode.

Examples

The following sample output displays active and total call information across the WebSocket IDs:

```
router#show voip stream-service connection
ID        Local IP:Port         Remote Hostname/IP:Port    Secure      Active Sessions
Total Sesions

68        10.65.125.186:30097   10.64.86.215:5022          No           10              10
66        10.65.125.186:41051   10.64.86.70:5067           Yes          1               1
30        10.65.126.206:46884   hdfwehdfgewjkgw...:8090    No           0               1

**Remote Hostname is truncated if it exceeds 15 characters.
-------------------------------------------------------------------------------------------
```

The table describes significant fields shown in this output.

Table 208: Show voip stream-service connection Field Descriptions

Local IP:Port	The IP address and port assigned to a WebSocket connection on CUBE.
Remote IP:Port	The IP address or hostname and corresponding port of the remote WebSocket server.
Active Calls	The total number of active calls on the WebSocket connection.
Total Calls	The total number of calls handled on this WebSocket connection.

Related Commands

Command	Description
show voip stream-service connection history	Displays information about all the closed WebSocket connections in CUBE.
show voip stream-service server <ip:port>	Displays information about the WebSocket connection based on WebSocket server IP and port.
show voip stream-service connection id <id>	Displays information about a WebSocket connection based on the WebSocket ID. Also, it displays all the forked call details.

show voip stream-service connection history

To display information about all the closed or stale WebSocket connections in Cisco Unified Border Element, use the **show voip stream-service connection history** command in privileged EXEC mode.

show voip stream-service connection history

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Bengaluru 17.6.1a	This command was introduced.

Usage Guidelines

Use this command to display the list of all WebSocket connections in closed or stale state. The number of total calls and the reason for WebSocket connection disconnect is also displayed.

Note For this CLI command output, a maximum of 100 entries is supported per server.

Examples

```
router#show voip stream-service connection history
Id     Local IP:Port        Remote IP:Port      Secure  Total   Disconnect Cause
                                                       Sessions
16     10.65.125.186:41167  10.64.86.215:5022   No      5       WS_IDLE_TIMEOUT_CLOSURE

33     10.65.125.186:11079  10.64.86.215:5022   Yes     10      WS_IDLE_TIMEOUT_CLOSURE

48     10.65.125.186:38169  10.64.86.70:5067    No      1       WS_IDLE_TIMEOUT_CLOSURE

**Remote Hostname is truncated if it exceeds 15 characters
```

The table describes significant fields shown in this output.

Table 209: Show voip stream-service connection history Field Descriptions

Local ip:port	The IP address and port assigned to a WebSocket connection on Cisco Unified Border Element.
Remote ip:port	The IP address and port of the remote WebSocket server.
Total Calls	The total number of calls handled on this WebSocket connection.
Disconnect Cause	The reason for the termination of WebSocket connection.

Related Commands

Command	Description
show voip stream-service connection	Displays information about the active WebSocket connections in Unified Border Element.

Command	Description
show voip stream-service server <ip:port>	Displays information about the WebSocket connection based on WebSocket server IP and port.
show voip stream-service connection id <id>	Displays information about a WebSocket connection based on the WebSocket ID. Also, it displays all the forked call details.

show voip stream-service connection id

To display detailed information about a specific WebSocket connection in Cisco Unified Border Element, use the **show voip stream-service connection id** *id* command in privileged EXEC mode.

show voip stream-service connection id *id*

Syntax Description

id	The ID associated with a WebSocket connection.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Bengaluru 17.6.1a	This command was introduced.
Cisco IOS XE Dublin 17.12.1a	Added support for GCM cipher suite negotiation.

Usage Guidelines

Use this command to display detailed information about a specific WebSocket connection. The information is provided based on the unique *id* associated with a WebSocket connection. The following are some of the details about the WebSocket connection displayed by the show command:

- WebSocket ID
- Total Call Count
- Active Call Count
- Server Address
- Local Address
- State
- Connection Timestamp
- Idle Timestamp
- Disconnect Cause
- Call Leg Details
- Secure
- TLS Version
- Cipher Suite
- Authorization Token

Examples

The following is a sample output for the command **show voip stream-service connection id** *id* for an active WebSocket connection.

```
router#show voip stream-service connection id 2
Id:2
```

```
Total call count:1
Active calls count:1
State: Active
Connected at: *Aug 21 20:34:43 UTC
Anchor leg cccallid        Data plane fork session id

2                          1
```

The following is a sample output for the command **show voip stream-service connection id** *id* for a disconnected WebSocket connection.

```
router#show voip stream-service connection id 16
Id:16
Total Calls:5
State: Disconnected
Connected at: *Aug 21 12:13:34 UTC
Disconnected at: *Aug 21 12:18:34 UTC
Disconnect Cause: WS_IDLE_TIMEOUT_CLOSURE
```

The following is a sample output for the command **show voip stream-service connection id** *id* for an idle WebSocket connection.

```
router#sh voip stream-service connection id 24
Id: 24
Total sessions: 1
Secure: No
Auth Token:
e2238f3a-e43c-3f54-a05a-dd2e4bd4631fe2238f3a-e43c-3f54-a05a-dd2e4bd4631fe2238f3a-e43c-3f54-a05a-dd2e...

Server Address: 8.43.24.49:2313
Local Address: 8.43.21.36:19631
Proxy : 8.43.24.189:8097
State: Disconnected
Connected at: *Oct 27 05:35:35 UTC
Disconnected at: *Oct 27 05:40:56 UTC
Disconnect Cause: WS_TCP_CONNECTION_CLOSURE
```

The following is a sample output for the command **show voip stream-service connection id** *id* for a secure WebSocket connection.

```
router#sh voip stream-service connection id 38
Id: 38
Total session count: 1
Active session count: 1
Secure: Yes
TLS Version: TLS1.2
Cipher Suite: AES128-SHA
Auth Token:
e2238f3a-e43c-3f54-a05a-dd2e4bd4631fe2238f3a-e43c-3f54-a05a-dd2e4bd4631fe2238f3a-e43c-3f54-a05a-dd2e...

Server Address: 8.43.24.49:2311
Local Address: 8.43.21.36:28469
Proxy : 8.43.24.189:8097
State: Active
Connected at: *Oct 27 05:42:27 UTC

Anchor leg cccallid        Data plane fork session id
       37                            3
```

The following is a sample output for the command **show voip stream-service connection id** *id* for a GCM specific cipher secure WebSocket connection:

```
router#show voip stream-service connection id 60
Id: 60
Total session count: 1
```

```
Active session count: 1
Secure: Yes
TLS Version: TLS1.2
Cipher Suite: ECDHE-RSA-AES256_GCM-SHA384
Auth Token: e2238f3a-e43c-3f54-a05a-dd2e4bd4631f
Server Address: 10.1.40.50:8051
Local Address: 10.2.10.10:52642
State: Active
Connected at: Feb 7 07:47:27 UTC

Anchor leg cccallid        Data plane fork session id
       58                              2
```

The table describes significant fields shown in this output.

Table 210: Show voip stream-service connection id <id> Field Descriptions

State	The current state of WebSocket connection (Active or Disconnected).
Id	The ID number associated with the WebSocket connection.
Active call count	The total number of active calls on the WebSocket connection.
Total call count	The total number of calls handled on this WebSocket connection.
Connected at	The timestamp at which the WebSocket connection was established.
Disconnected at	The timestamp when WebSocket connection was terminated. It's displayed only if the WebSocket connection is disconnected.
Disconnect Cause	The cause for termination of WebSocket connection.
Idle Since	The duration (in minutes) for which the WebSocket connection is idle.

Related Commands

Command	Description
show voip stream-service connection	Displays information about the active WebSocket connections in Unified Border Element.
show voip stream-service connection history	Displays information about all the closed WebSocket connections in Unified Border Element.
show voip stream-service server <ip:port>	Displays information about the WebSocket connection based on WebSocket server IP and port.

show voip stream-service server

To display information about all the WebSocket connections for a specific speech server ip and port, use the **show voip stream-service server** *ip:port* command in privileged EXEC mode.

show voip stream-service server *ip:port*

Syntax Description

ip:port	The IP address and port details associated with a speech server.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Bengaluru 17.6.1a	This command was introduced.

Usage Guidelines

Use this command to display detailed information about the WebSocket connections specific to a speech server ip address and port. Detailed information about WebSocket connections such as WebSocket ID, state (active or disconnected), and total number of calls received on the WebSocket connection are displayed. If the WebSocket connection is in **Active** state, information is provided on the number of active calls. If the WebSocket connection is in **Disconnected** state, the disconnect cause is specified.

Examples

The following is a sample output for the command **show voip stream-service connection server** *ip:port* for an active WebSocket connection.

```
router#show voip stream-service server 10.64.86.70:5067
Total 2 connections found
ID        State           Secure   Total Calls  Active Session/Disconnect Cause
66        Active          Yes      1            1
48        Disconnected    No       1            WS_IDLE_TIMEOUT
```

The table describes significant fields shown in this output.

Table 211: Show voip stream-service connection id <id> Field Descriptions

State	The current state of WebSocket connection (Active or Disconnected).
Id	The ID number associated with the WebSocket connection.
Active Calls	The total number of active calls on the WebSocket connection.
Total Calls	The total number of calls handled on this WebSocket connection.
Disconnect Cause	The cause for termination of WebSocket connection.

Related Commands

Command	Description
show voip stream-service connection	Displays information about the active WebSocket connections in Unified Border Element.

Command	Description
show voip stream-service connection history	Displays information about all the closed WebSocket connections in Unified Border Element.
show voip stream-service connection id <id>	Displays information about a WebSocket connection based on the WebSocket ID. Also, it displays all the forked call details.

show voip stream-service statistics

To display statistical information about WebSocket connections in Cisco Unified Border Element, use the **show voip stream-service statistics** command in privileged EXEC mode.

show voip stream-service statistics

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Bengaluru 17.6.1a	This command was introduced.

Usage Guidelines

The following are some of the statistical information about the WebSocket connection that is displayed by the command:

- Active connections
- Active forked sessions
- Total connections created
- Total forked sessions
- Connection closures
- Message statistics

Examples

The following is a sample output for the command **show voip stream-service statistics** .

```
router#show voip stream-service statistics
Active connections:          0
Active forked sessions:      3
Total connections created:   3
Total forked sessions:       8

Connection closures:
HTTP failures:               0
TCP failures:                0
TLS failures:                0
Remote WebSocket closures:   0
TCP connection closures:     1
Idle-timeouts:              1

Message statistics:
WS_CREATE_REQ:               3
WS_CREATE_RSP_OK:            3
WS_CREATE_RSP_FAIL:          0
WS_CLOSE_REQ:                1
WS_CLOSE_RSP:                1
WS_DOWN:                     1
WS_DOWN_ALL:                 1
```

The table describes fields that are shown in this output.

Table 212: Field Descriptions

Active connections	Number of active WebSocket connections.
Active forked sessions	Number of active forked sessions.
Total connections created	Total number of WebSocket connections created on CUBE.
Total forked sessions	Total number of forked sessions on CUBE.
Connection closures	Information about connection closures that are related to WebSockets on CUBE.
HTTP failures	Number of HTTP connection setup failures.
TCP failures	Number of TCP connection setup failures.
TLS failures	Number of Transport Layer Security (TLS) connection setup failures.
Remote WebSocket closures	Number of WebSocket connections that are closed remotely.
TCP connection closures	Number of TCP connection closures, including local and remote closures.
Idle-timeouts	Number of TCP connections closed by CUBE due to idle timeout.
Message statistics	Statistics about messages and responses for a WebSocket connection.
WS_CREATE_REQ	Count of requests for creating WebSocket connection.
WS_CREATE_RSP_OK	Count of responses for WebSocket connection requests that are successful.
WS_CREATE_RSP_FAIL	Count of responses for WebSocket connection requests that are unsuccessful.
WS_CLOSE_REQ	Count of requests for WebSocket connection closure.
WS_CLOSE_RSP	Count of responses for WebSocket connection closure.
WS_DOWN	Count of events in which WebSocket connection is down, including remote and local closures.
WS_DOWN_ALL	Count of all WebSocket down events during switchover. All WebSocket connections are closed during a Forwarding Plane (FP) Switchover. Each count represents one FP switchover.

Related Commands

Command	Description
clear voip stream-service statistics	Clears global WebSocket connections for CUBE.
show voip stream-service connection history	Displays information about all the closed WebSocket connections in CUBE.
show voip stream-service server <ip:port>	Displays information about the Server IP and port of a WebSocket connection.

show voip trace

To display the VoIP trace information for SIP calls received and sent on CUBE, use the **show voip trace** command in privileged EXEC mode.

show voip trace { **all** | **call-id** *identifier* | **correlator** *identifier* | **cover-buffers** | **session-id** *identifier* | **sip-call-id** *identifier* | **statistics** [**detail**] | **tenant** *identifier* }

Syntax Description

all	Displays all the traces for both active and disconnected calls.
call-id	Displays detailed call information for a call based on the CCAPI call ID.
correlator	Displays detailed call information for a call based on the VOIP FPI correlator ID.
cover-buffers	Displays the summary of cover buffers for all the buffers in the memory.
session-id	Displays detailed call information for a call based on the SIP session-ID.
sip-call-id	Displays detailed call information for a call based on the SIP call ID in a SIP INVITE message.
statistics	Displays the VoIP trace statistics for incoming and outgoing calls.
detail	(Optional) Displays the detailed VoIP trace statistics for incoming and outgoing calls.
tenant	Displays detailed call information for calls based on tenant tags.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Bengaluru 17.5.1a	The **show voip trace** command for SIP messages is enhanced to display the source and destination IP addresses.
Cisco IOS XE Cupertino 17.8.1a	The **show voip trace** command: • Enhanced to display the tenant tag. • Supports tenant based filtering.
Cisco IOS XE Dublin 17.12.1a	The **show voip trace** command for SIP messages is enhanced to display cause code in the cover buffer.

Usage Guidelines

Use **show voip trace** command to display the statistics, details of the memory expansion counters for message buffers to store additional logs, and information from trace buffers for all SIP call legs. When VoIP Trace is enabled (no shutdown), use **show voip trace** command to display information for all SIP call legs in the trace buffers.

Starting from Cisco IOS XE Dublin 17.12.1a, VoIP trace format is updated to include cause-code information display in the cover buffer.

Note

- If the count of cover buffers exceeds the threshold value 200, the router performance reduces for **show voip trace all** command. Use **show voip trace cover-buffers** and other filter commands instead of **show voip trace all**.
- To change the Timestamps displayed in the VoIP trace, configure the following:

```
router(config)# monitor event-trace timestamps datetime ?
  localtime      Use local time zone for timestamps
  msec           Include milliseconds in timestamp
  show-timezone  Add time zone information to timestamp
```

Examples

The following sample output displays voip trace information for cover-buffers. The tenant tag can be acquired using the **show voip trace cover-buffers**.

```
router# show voip trace cover-buffers
------------------ Cover Buffer ---------------
Search-key       = sipp:8765:121
  Timestamp      = Nov  9 04:47:39.427
  Buffer-Id      = 1
  CallID         = 121
  Peer-CallID    = 122
  Correlator     = 7
  Called-Number  = 8765
  Calling-Number = sipp
  SIP CallID     = 1-28575@8.41.17.71
  SIP Session ID = b91e516ba375585aae54b3f0abdd6f13
  GUID           = 87954DCE80A7
  Tenant         = 100
```

The following is a sample output of the **show voip trace cover-buffers** command displaying cause-code, which is supported from Cisco IOS XE Dublin 17.12.1a release:

```
Device# show voip trace cover-buffers
------------------ Cover Buffer ---------------
Search-key       = 808808:6666:4
  Timestamp      = Apr 27 09:54:54.491
  CallID         = 4
  Peer-CallID    = 5
  Correlator     = NA
  Called-Number  = 6666
  Calling-Number = 808808
  SIP CallID     = 1-18630@10.1.40.50
  SIP SessionID  =
  GUID           = 651A3C548005
  Tenant         = 0
  Cause-code     = recovery on timer expiry (102)
-----------------------------------------------
```

The following sample output displays a tenant based filtering for voip trace:

```
router# show voip trace ?
  all            Display all VoIP Traces
  call-id        Filter traces based on Internal Call Id
  correlator     Filter traces based on FPI Correlator
  cover-buffers  Display the summary of all cover buffers
  session-id     Filter traces based on SIP Session ID
  sip-call-id    Filter traces based on SIP Call Id
```

```
  statistics     Display statistics for VoIP Trace
  tenant         Filter traces based on tenant tags

vCUBE1# show voip trace tenant ?
 <0-10000>  Tenant tag to be matched, tag 0 indicates calls associated with no tenant (max
 of 10 tags)

vCUBE1# show voip trace tenant 1 ?
 <0-10000>  Tenant tag to be matched, tag 0 indicates calls associated with no tenant (max
 of 10 tags)
<cr>            <cr>

vCUBE1# show voip trace tenant  0 1 2 3 4 5 6 7 8 9 ?
<cr>            <cr>
```

Examples

The following sample output displays voip trace information for a call with call-id 121. The call id can be acquired using the **show voip trace cover-buffers**.

The following sample output displays voip trace information for a IPv6 call:

```
router# show voip trace call-id 39
------------------ Cover Buffer ---------------
Search-key       = sipp:5678:39
  Timestamp      = *Dec 25 22:09:00.068
  Buffer-Id      = 1
  CallID         = 39
  Peer-CallID    = 40
  Correlator     = 16
  Called-Number  = 5678
  Calling-Number = sipp
  SIP CallID     = 1-8921@2001:420:54ff:13::312:71
  SIP Session ID = d921890ab3aa557891b6dd2888b0602b
  GUID           = 9FF305D88076
-----------------------------------------------
2232: *Dec 25 22:09:00.068: //39/9FF305D88076/CUBE_VT/SIP/Msg/ccsipDisplayMsg:
Received: SIP UDP message from [2001:420:54FF:13::312:71]:10000 to
[2001:420:54FF:13::652:23]:5060
INVITE sip:5678@[2001:420:54ff:13::652:23]:5060 SIP/2.0
Via: SIP/2.0/UDP [2001:420:54ff:13::312:71]:10000;branch=z9hG4bK-8921-1-0
From: sipp <sip:sipp@[2001:420:54ff:13::312:71]:10000>;tag=8921SIPpTag001
To: sut <sip:5678@[2001:420:54ff:13::652:23]:5060>
Call-ID: 1-8921@2001:420:54ff:13::312:71
CSeq: 1 INVITE
Contact: sip:sipp@[2001:420:54ff:13::312:71]:10000

Max-Forwards: 70
Subject: Performance Test
Content-Type: application/sdp
Content-Length:   161

v=0
o=user1 53655765 2353687637 IN IP6 [2001:420:54ff:13::312:71]
s=-
c=IN IP6 2001:420:54ff:13::312:71
t=0 0
m=audio 6001 RTP/AVP 0
a=rtpmap:0 PCMU/8000

2234: *Dec 25 22:09:00.067: //39/9FF305D88076/CUBE_VT/SIP/FSM/SPI-State-Change: Current
State = STATE_NONE, Next State = STATE_IDLE, Current Sub-State = STATE_NONE, Next Sub-State
 = STATE_NONE
2235: *Dec 25 22:09:00.069: //39/9FF305D88076/CUBE_VT/SIP/MISC/Matched Dialpeer: Dir:Inbound,
 Peer-Tag:  3
```

```
2236: *Dec 25 22:09:00.069: //39/9FF305D88076/CUBE_VT/SIP/FSM/Offer-Answer: Event =
E_SIP_INVITE_SDP_RCVD, Current State = S_SIP_EARLY_DIALOG_IDLE, Next State =
S_SIP_EARLY_DIALOG_OFFER_RCVD
2237: *Dec 25 22:09:00.069: //39/9FF305D88076/CUBE_VT/SIP/FSM/IWF: Event =
E_SIP_IWF_EV_RCVD_SDP, Current State = S_SIP_IWF_SDP_IDLE, Next State =
S_SIP_IWF_SDP_RCVD_AWAIT_PEER_EVENT
2238: *Dec 25 22:09:00.070: //39/9FF305D88076/CUBE_VT/SIP/MISC/Media Stream Parameters:
Stream Type = voice-only, Stream State = STREAM_ADDING Negotiated Codec = g711ulaw, Negotiated
 DTMF Type = inband-voice, Stream Index =  1
2239: *Dec 25 22:09:00.071: //39/9FF305D88076/CUBE_VT/SIP/API:
cc_api_update_interface_cac_resource (0)
2240: *Dec 25 22:09:00.071: //39/9FF305D88076/CUBE_VT/SIP/API: voip_rtp_allocate_port (8020)
2241: *Dec 25 22:09:00.071: //39/9FF305D88076/CUBE_VT/SIP/MISC/Media Stream Parameters:
Stream Type = voice-only, Stream State = STREAM_ADDING Negotiated Codec = g711ulaw, Negotiated
 DTMF Type = inband-voice, Stream Index =  1
2242: *Dec 25 22:09:00.071: //39/9FF305D88076/CUBE_VT/SIP/API:
cc_api_call_setup_ind_with_callID (0)
2243: *Dec 25 22:09:00.072: //39/9FF305D88076/CUBE_VT/SIP/FSM/SPI-State-Change: Current
State = STATE_IDLE, Next State = STATE_RECD_INVITE, Current Sub-State = STATE_NONE, Next
Sub-State = STATE_NONE
2248: *Dec 25 22:09:00.073: //39/9FF305D88076/CUBE_VT/SIP/FSM/IWF: Event =
E_SIP_IWF_EV_SET_MODE, Current State = CNFSM_CONTAINER_STATE, Next State =
CNFSM_NO_STATE_CHANGE
2249: *Dec 25 22:09:00.074: //39/9FF305D88076/CUBE_VT/SIP/API: voip_rtp_create_session (0)
2250: *Dec 25 22:09:00.074: //39/9FF305D88076/CUBE_VT/SIP/API: voip_rtp_set_non_rtp_call
(0)
2251: *Dec 25 22:09:00.074: //39/9FF305D88076/CUBE_VT/SIP/API: voip_rtp_update_callinfo (0)
2252: *Dec 25 22:09:00.074: //39/9FF305D88076/CUBE_VT/SIP/FSM/Event-Action: Event =
SIPSPI_EV_CC_CALL_PROCEEDING, Current State = STATE_RECD_INVITE
2272: *Dec 25 22:09:00.077: //39/9FF305D88076/CUBE_VT/SIP/Msg/ccsipDisplayMsg:
Sent: SIP UDP message from [2001:420:54FF:13::652:23]:5060 to [2001:420:54FF:13::312:71]:10000

SIP/2.0 100 Trying
Via: SIP/2.0/UDP [2001:420:54ff:13::312:71]:10000;branch=z9hG4bK-8921-1-0
From: sipp <sip:sipp@[2001:420:54ff:13::312:71]:10000>;tag=8921SIPpTag001
To: sut <sip:5678@[2001:420:54ff:13::652:23]:5060>
Date: Fri, 25 Dec 2020 22:09:00 GMT
Call-ID: 1-8921@2001:420:54ff:13::312:71
CSeq: 1 INVITE
Allow-Events: telephone-event
Server: Cisco-SIPGateway/IOS-17.5.20201117.131853
Session-ID: 00000000000000000000000000000000;remote=e714644e7e385e90a1d75a34855ef73a
Content-Length: 0
```

The table describes significant fields that are shown in this output.

Table 213: Show voip trace Field Descriptions

Search-key	Displays the Search-key of the cover buffer. The Search-key value is the **Calling number:Called number:call ID**.
Timestamp	Displays the creation time of the cover buffer.
Buffer-Id	Displays the Buffer ID of the cover buffer.
CallID	Displays the Call ID of the respective call leg present in the cover buffer.
Peer-CallID	Displays the Peer Call ID of the respective call leg present in the cover buffer.
Correlator	Displays the Correlator ID of the respective call leg present in the cover buffer.

Called-Number	Displays the Called Number of the respective call leg present in the cover buffer.
Calling-Number	Displays the Calling Number of the respective call leg present in the cover buffer.
SIP CallID	Displays the SIP Call ID of the respective call leg present in the cover buffer.
SIP-Session ID	Displays the SIP Session ID of respective call leg present in the cover buffer.
GUID	Displays the GUID of the respective call leg present in the cover buffer.
Anchor Leg	Indicates whether the call leg in the buffer acts as the Anchor leg during recording.
Forked Leg	Indicates whether the call leg in the buffer acts as the Forked leg during recording.
Associated CallID's	Displays the Call IDs associated with forking.
tenant	Displays the tenant tag of the respective call leg present in the cover buffer.
cause-code	Starting from Cisco IOS XE Dublin 17.12.1a, displays the call success or call failure cause-code in the cover buffer for a call leg.

The following is sample output of show voip trace statistics after disabling voip trace:

```
router# show voip trace statistics
VoIP Trace Statistics
Tracing status             : DISABLED
router#
```

The following is sample output of show voip trace statistics after missing 50 call legs due to memory exhaustion:

```
router# show voip trace statistics
VoIP Trace Statistics
Tracing status             : ENABLED at Jun 15 10:01:24.911
Memory limit configured    : 10485760 bytes
Memory consumed            : 10039760 bytes (95%)
Total call legs dumped     : 3
Oldest trace dumped        : Jun 15 10:03:31.121, Search-key: sipp:799:200
Latest trace dumped        : Jun 15 10:25:03.616, Search-key: sipp:123:293
Total call legs captured   : 243
Total call legs available  : 116
Oldest trace available     : Jun 15 10:19:31.844, Search-key: sipp:799:125
Latest trace available     : Jun 15 10:25:03.616, Search-key: sipp:123:293
Total traces missed        : 50
router#
```

The table describes significant fields that are shown in this output.

Table 214: Show voip trace statistics Field Descriptions

Tracing status	Displays the timestamp, and the tracing status is enabled or disabled.
Memory limit configured	Displays the total memory-limit.
Memory consumed	Displays the current memory that is consumed by the buffers. The memory that is consumed is also displayed in percentage.
Total call legs dumped	Displays the total marked buffers that are dumped in the logging buffer.

Oldest trace dumped	Displays the timestamp and the search key of the first buffer dumped.
Latest trace dumped	Displays the timestamp and the search key of the newest buffer dumped.
Total call legs captured	Displays the total call legs that are captured after the trace is enabled.
Total call legs available	Displays the total call legs available in the history.
Oldest trace available	Displays the timestamp and the search key of the oldest buffer.
Latest trace available	Displays the timestamp and search key of the latest buffer.
Total traces missed	Displays the number of call legs missed due to memory-limit.

The following is a sample output of the **show voip trace cover-buffers**:

```
router# show voip trace cover-buffers
------------------ Cover Buffer ---------------
Search-key       = sipp:799:1
  Timestamp      = *Jun 25 14:55:35.318
  Buffer-Id      = 1
  CallID         = 1
  Peer-CallID    = 2
  Correlator     = NA
  Called-Number  = 799
  Calling-Number = sipp
  SIP CallID     = 1-630@10.64.86.70
  SIP Session ID =
  GUID           = C250D2778002
-----------------------------------------------
------------------ Cover Buffer ---------------
Search-key       = sipp:799:2
  Timestamp      = *Jun 25 14:55:35.338
  Buffer-Id      = 2
  CallID         = 2
  Peer-CallID    = 1
  Correlator     = NA
  Called-Number  = 799
  Calling-Number = sipp
  SIP CallID     = C254A2BD-B62A11EA-8008BF9C-3C4C9D37@8.43.21.71
  SIP Session ID =
  GUID           = C250D2778002
-----------------------------------------------
```

The following is sample output of the **show voip trace statistics detail**:

```
router# show voip trace statistics detail
VoIP Trace Statistics
Tracing status             : ENABLED at Jun 29 07:48:56.973
Memory limit configured    : 1048576000 bytes
Memory consumed            : 1000006016 bytes (95%)
Total call legs dumped     : 7298
Oldest trace dumped        : Jun 29 07:57:30.503, Search-key: 205521:405521:10043
Latest trace dumped        : Jun 29 09:41:44.251, Search-key: 218221:418221:69148
Total call legs captured   : 69148
Total call legs available  : 57851
Oldest trace available     : Jun 29 08:41:06.687, Search-key: 205521:405521:11043
Latest trace available     : Jun 29 10:13:21.091, Search-key: 218221:418221:69148
Total traces missed        : 0
```

```
Buffer Expansion Counters  :
============================================================
        Expansions      MSG     FSM     API     MISC
============================================================
             1          3517    0       0       0
             2          1441    0       0       0
             3          29      0       0       0
             4          629     0       0       0
             5          0       0       0       0
             6          0       0       0       0
             7          0       0       0       0
             8          0       0       0       0
             9          0       0       0       0
             10+        0       0       0       0
============================================================
```

The table describes significant fields that are shown in this output.

Table 215: Show detailed voip trace statistics detail Field Descriptions

Expansions	Displays the number of memory expansions that are performed to store the additional logs. For example, CUBE performed 1 message buffer expansion for storing SIP messages for 3517 cover buffers or 4 message buffer expansions for storing SIP messages for 629 cover buffers.
MSG	Displays the number of times the SIP message trace buffers have expanded.
FSM	Displays the number of times the Finite (Call) State Machine call trace buffers have expanded.
API	Displays the number of times the Functional call trace buffers have expanded.
Misc	Displays the number of times the Miscellaneous call trace buffers have expanded.

Examples

If you configure the CLI command **shutdown** in trace configuration sub-mode, the show command doesn't display trace information. The following is a sample show command output for the scenario:

```
router#config terminal
Enter configuration commands, one per line.  End with CNTL/Z.
router(config)#voice service voip
router(conf-voi-serv)#trace
router(conf-serv-trace)#shutdown
router(conf-serv-trace)#exit
router(conf-voi-serv)#exit
router(config)#end
router#show voip trace all | sec Cover Buffer
router#show voip trace all
                No Data to Display !!

router#show voip trace call-id 7
                No records for the filter specified !!

router#
```

Related Commands

Command	Description
trace	Enables the VoIP trace serviceability framework for SIP calls in CUBE.

Command	Description
shutdown (trace)	Disables the VoIP trace serviceability framework in CUBE.
memory-limit (trace)	Defines the memory limit for storing VoIP trace information.

show voip trunk group

To display the internal list of voip trunk groups, use the **show voip trunk group** command in user EXEC or privileged EXEC mode.

show voip trunk group

Syntax Description

This command has no arguments or keywords.

Command Default

Command Modes

User EXEC (>)
Privileged EXEC (#)

Command History

Release	Modification
15.2(2)T	This command was introduced.

Usage Guidelines

Use this command to display VOIP trunk groups.

Examples

The following example is a sample output from the **show voip trunk group** command.

```
Router# show voip trunk group

=====================================================
name: 1
protocol: cisco
ip: 1.3.45.2
xsvc: TRUE
```

Related Commands

Command	Description
voip trunk group	Specifies a VOIP trunk group.

show vrm active_calls

To display active-only voice calls either for a specific voice feature card (VFC) or for all VFCs, use the **show vrm active_calls**command in privileged EXEC mode.

show vrm active_calls {*dial-shelf-slot-number* | **all**}

Syntax Description

dial -shelf-slot-number	Slot number of the dial shelf. Range is from 0 to 13.
all	Displays list of all active calls for VFC slots.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.0(7)T	This command was introduced on the Cisco AS5800.

Usage Guidelines

Use this command to display active-only voice calls either for a specific VFC or for all VFCs. Each active call occupies a block of information describing the call. This information provides basically the same information as the **show vrm vdevice** command.

Examples

The following is sample output from this command specifying a dial-shelf slot number:

```
Router# show vrm active_calls 6
slot =  6 virtual voice dev (tag) =  61 channel id = 2
capabilities list map = 9FFF
last/current codec loaded/used = None
TDM timeslot = 241
Resource (vdev_common) status = 401 means :active others
tot ingress data =  24
tot ingress control  = 1308
tot ingress data drops  = 0
tot ingress control drops  = 0
tot egress data  = 22051
tot egress control  = 1304
tot egress data drops  = 0
tot egress control drops  = 0
slot =  6 virtual voice dev (tag) =  40 channel id = 2
capabilities list map = 9FFF
last/current codec loaded/used = None
TDM timeslot = 157
Resource (vdev_common) status = 401 means :active others
```

The table below describes significant fields shown in this output.

Table 216: show vrm active_calls Field Descriptions

Field	Description
slot	Slot where the voice card is installed.

Field	Description
virtual voice dev (tag)	ID number of the virtual voice device.
channel id	ID number of the channel associated with this virtual voice device.
capability list map	Bitmaps for the codec supported on that DSP channel. Values are the following: • CC_CAP_CODEC_G711U: 0x1 • CC_CAP_CODEC_G711A: 0x2 • CC_CAP_CODEC_G729IETF: 0x4 • CC_CAP_CODEC_G729a: 0x8 • CC_CAP_CODEC_G726r16: 0x10 • CC_CAP_CODEC_G726r24: 0x20 • CC_CAP_CODEC_G726r32: 0x40 • CC_CAP_CODEC_G728: 0x80 • CC_CAP_CODEC_G723r63: 0x100 • CC_CAP_CODEC_G723r53: 0x200 • CC_CAP_CODEC_GSM: 0x400 • CC_CAP_CODEC_G729b: 0x800 • CC_CAP_CODEC_G729ab: 0x1000 • CC_CAP_CODEC_G723ar63: 0x2000 • CC_CAP_CODEC_G723ar53: 0x4000 • CC_CAP_CODEC_G729: 0x8000
last/current codec loaded/used	Last codec loaded or used.
TDM time slot	Time-division-multiplexing time slot.
Resource (vdev_common) status	Current status of the VFC.
tot ingress data	Total amount of data (number of packets) sent from the PSTN side of the connection to the VoIP side of the connection.
tot ingress control	Total number of control packets sent from the PSTN side of the connection to the VoIP side of the connection.
tot ingress data drops	Total number of data packets dropped from the PSTN side of the connection to the VoIP side of the connection.
tot ingress control drops	Total number of control packets dropped from the PSTN side of the connection to the VoIP side of the connection.

Field	Description
tot egress data	Total amount of data (number of packets) sent from the VoIP side of the connection to the PSTN side of the connection.
tot egress control	Total number of control packets sent from the VoIP side of the connection to the PSTN side of the connection.
tot egress data drops	Total number of data packets dropped from the VoIP side of the connection to the PSTN side of the connection.
tot egress control drops	Total number of control packets dropped from the VoIP side of the connection to the PSTN side of the connection.

Related Commands

Command	Description
show vrm vdevices	Displays detailed information for a specific DSP or a brief summary display for all VFCs.

show vrm vdevices

To display detailed information for a specific digital signal processor (DSP) or summary information for all voice feature cards (VFCs), use the **show vrm vdevices**command in privileged EXEC mode.

show vrm vdevices {**vfc-slot-number voice-device-number** | **alarms** [**vfc-slot-number-for-alarms**] | **summary**}

Syntax Description

vfc -slot-number	Slot number of the VFC. Range is from 0 to 11.
voice -device-number	DSP number. Range is from 1 to 96.
alarms	DSP alarm statistics for all DSPs on all slots or specified slots.
vfc -slot-number-for-alarms	(Optional) Slots for which you need alarm information. If no slots are specified, alarm information for all slots is displayed.
summary	Synopsis of voice feature card DSP mappings, capabilities, and resource states.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.0(7)T	This command was introduced on the Cisco AS5800.
12.2(11)T	The **alarms** keyword and *vfc-slot-number-for-alarms* argument were added.

Usage Guidelines

Use this command to display detailed information for a specific DSP or a brief summary for all VFCs. The display provides information such as the number of channels, channels per DSP, bitmap of digital signal processor modules (DSPMs), DSP alarm statistics, and version numbers. This information is useful in monitoring the current state of your VFCs.

The display for a specific DSP provides information on the codec that each channel is using, if active, or on the codec that was last used and whether the channel is not currently sending cells. It also displays the state of the resource. In most cases, if there is an active call on that channel, the resource should be marked active. If the resource is marked as reset or bad, this may be an indication of a response loss for the VFC on a reset request. If this condition persists, you might experience a problem with the communication link between the router shelf and the VFC.

Examples

The following is sample output from this command specifying dial-shelf slot number and DSP number. In this particular example, the call is active so the statistics displayed are for this active call. If no calls are currently active on the device, the statistics would be for the previous (or last active) call.

```
Router# show vrm vdevices 6 1
slot =  6 virtual voice dev (tag) =  1 channel id = 1
capabilities list map = 9FFF
last/current codec loaded/used = None
TDM timeslot = 0
```

```
Resource (vdev_common) status = 401 means :active others
tot ingress data =  101
tot ingress control  = 1194
tot ingress data drops  = 0
tot ingress control drops  = 0
tot egress data  = 39722
tot egress control  = 1209
tot egress data drops  = 0
tot egress control drops  = 0
slot =  6 virtual voice dev (tag) =  1 channel id = 2
capabilities list map = 9FFF
last/current codec loaded/used = None
TDM timeslot = 1
Resource (vdev_common) status = 401 means :active others
tot ingress data =  21
tot ingress control  = 1167
tot ingress data drops  = 0
tot ingress control drops  = 0
tot egress data  = 19476
tot egress control  = 1163
tot egress data drops  = 0
tot egress control drops  = 0
```

The table below describes significant fields shown in this output.

Table 217: show vrm vdevices Field Descriptions

Field	Description
slot	Slot in which the voice card is installed.
virtual voice dev (tag)	ID number of the virtual voice device.
channel id	ID number of the channel that is associated with this virtual voice device.

Field	Description
capabilities list map	Bitmaps for the codec supported on that DSP channel. Values are as follows: • CC_CAP_CODEC_G711U: 0x1 • CC_CAP_CODEC_G711A: 0x2 • CC_CAP_CODEC_G729IETF: 0x4 • CC_CAP_CODEC_G729a: 0x8 • CC_CAP_CODEC_G726r16: 0x10 • CC_CAP_CODEC_G726r24: 0x20 • CC_CAP_CODEC_G726r32: 0x40 • CC_CAP_CODEC_G728: 0x80 • CC_CAP_CODEC_G723r63: 0x100 • CC_CAP_CODEC_G723r53: 0x200 • CC_CAP_CODEC_GSM: 0x400 • CC_CAP_CODEC_G729b: 0x800 • CC_CAP_CODEC_G729ab: 0x1000 • CC_CAP_CODEC_G723ar63: 0x2000 • CC_CAP_CODEC_G723ar53: 0x4000 • CC_CAP_CODEC_G729: 0x8000 • CC_CAP_CODEC_GSMEFR: 0x40000 • CC_CAP_CODEC_T38FAX: 0x10000
last/current codec loaded/used	Last codec loaded or used.
TDM timeslot	Time-division-multiplexing time slot.

Field	Description
Resource (vdev_common) status	Current status of the VFC. Values are as follows: • FREE = 0x0000 • ACTIVE_CALL = 0x0001 • BUSYOUT_REQ = 0x0002 • BAD = 0x0004 • BACK2BACK_TEST = 0x0008 • RESET = 0x0010 • DOWNLOAD_FILE = 0x0020 • DOWNLOAD_FAIL = 0x0040 • SHUTDOWN = 0x0080 • BUSY = 0x0100 • OIR = 0x0200 • HASLOCK = 0x0400 /* vdev_pool has locked port */ • DOWNLOAD_REQ = 0x0800 • RECOVERY_REQ = 0x1000 • NEGOTIATED = 0x2000 • OOS = 0x4000
tot ingress data	Total amount of data (number of packets) sent from the public switched telephone network (PSTN) side of the connection to the VoIP side of the connection.
tot ingress control	Total number of control packets sent from the PSTN side of the connection to the VoIP side of the connection.
tot ingress data drops	Total number of data packets dropped from the PSTN side of the connection to the VoIP side of the connection.
tot ingress control drops	Total number of control packets dropped from the PSTN side of the connection to the VoIP side of the connection.
tot egress data	Total amount of data (number of packets) sent from the VoIP side of the connection to the PSTN side of the connection.
tot egress control	Total number of control packets sent from the VoIP side of the connection to the PSTN side of the connection.
tot egress data drops	Total number of data packets dropped from the VoIP side of the connection to the PSTN side of the connection.

Field	Description
tot egress control drops	Total number of control packets dropped from the VoIP side of the connection to the PSTN side of the connection.

The following sample output displays alarm statistics for slot 6 of the DSP.

```
Router# show vrm vdevices alarms 6
----------------------ALARM STATISTICS FOR SLOT 6 ------------------------
TAG Mod DSP Chn OperStat  AlmCnt   AlmTime     AlmCause     AlmText
--------------------------------------------------------------------------
1   1   1   1   READY CD  0        0           1
                2   READY CD  0        0           1
2   1   2   1   READY CD  0        0           1
                2   READY CD  0        0           1
3   1   3   1   READY CD  0        0           1
                2   READY CD  0        0           1
4   1   4   1   READY CD  0        0           1
                2   READY CD  0        0           1
5   1   5   1   READY CD  0        0           1
                2   READY CD  0        0           1
6   1   6   1   READY CD  0        0           1
                2   READY CD  0        0           1
++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++
7   2   1   1   READY CD  0        0           1
                2   READY CD  0        0           1
8   2   2   1   READY CD  0        0           1
                2   READY CD  0        0           1
9   2   3   1   READY CD  0        0           1
                2   READY CD  0        0           1
10  2   4   1   READY CD  0        0           1
!
94  16  4   1   READY CD  0        0           1
                2   READY CD  0        0           1
95  16  5   1   READY CD  0        0           1
                2   READY CD  0        0           1
96  16  6   1   READY CD  0        0           1
                2   READY CD  0        0           1
++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++
```

The table below describes significant fields shown in this output.

Table 218: show vrm vdevices alarms Field Descriptions

Field	Description
TAG	Logical tag number.
Mod	DSP module number.
DSP	DSP number within the module.
Chn	Channel number for the DSP within the module.
OperStat	Operational status of the channel.
AlmCnt	Alarm count since bootup on that channel.
AlmTime	Time at which last alarm message was received.

Field	Description
AlmCause	Cause of last alarm message received.
AlmText	Text message corresponding to the last alarm message.
Possible Values for the Operational Status of the Channel (OperStat)	
RESET	RESET state.
DOWN	DOWN state.
READY CR	CORE READY state.
READY CD	CODEC READY state.
IDLE V	VOICE IDLE state.
IDLE FAX	FAX IDLE state.
READY V	VOICE READY state.
READY FX	FAX READY state.
READY D	DTMF READY state.
UNKNOWN	UNKNOWN state.

The following is sample output from this command specifying a summary list. In the "Voice Device Mapping" area, the "C_Ac" column indicates the number of active calls for a specific DSP. If there are any nonzero numbers under the "C_Rst" and/or "C_Bad" column, a reset request was sent, but it was lost; this could mean a faulty DSP.

```
Router# show vrm vdevices summary
*********************************************************
******summary of voice devices for all voice cards*********
*********************************************************
slot = 6 major ver = 0 minor ver = 1 core type used = 2
number of modules = 16 number of voice devices (DSPs) = 96
chans per vdevice = 2 tot chans = 192 tot active calls = 178
module presense bit map = FFFF tdm mode = 1 num_of_tdm_timeslots = 384
auto recovery is on
number of default voice file (core type images) = 2
file 0 maj ver = 0 min ver = 0 core_type = 1
trough size = 2880 slop value = 0 built-in codec bitmap = 0
loadable codec bitmap = 0 fax codec bitmap = 0
file 1 maj ver = 3 min ver = 1 core_type = 2
trough size = 2880 slop value = 1440 built-in codec bitmap = 40B
loadable codec bitmap = BFC fax codec bitmap = 7E
-------------------Voice Device Mapping-----------------------
Logical Device (Tag)  Module#  DSP#  C_Ac  C_Busy  C_Rst  C_Bad
-------------------------------------------------------------
1                     1        1     2     0       0      0
2                     1        2     2     0       0      0
3                     1        3     2     0       0      0
4                     1        4     2     0       0      0
5                     1        5     2     0       0      0
```

```
6                       1       6       2       0       0       0
++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++
7                       2       1       2       0       0       0
8                       2       2       2       0       0       0
9                       2       3       2       0       0       0
10                      2       4       1       0       0       0
11                      2       5       2       0       0       0
12                      2       6       1       0       0       0
.
.
.
91                      16      1       2       0       0       0
92                      16      2       2       0       0       0
93                      16      3       1       0       0       0
94                      16      4       2       0       0       0
95                      16      5       2       0       0       0
96                      16      6       2       0       0       0
++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++
Total active call channels = 178
Total busied out channels = 0
Total channels in reset = 0
Total bad channels = 0
Note :Channels could be in multiple states
```

The table below describes significant fields shown in this output.

Table 219: show vrm vdevices summary Field Descriptions

Field	Description
slot	Slot number in which the VFC is installed.
major ver	Major version of firmware running on the VFC.
minor ver	Minor version of firmware running on the VFC.
core type used	Type of DSPware in use. Values are as follows: • 1 = UBL (boot loader) • 2 = high complexity core • 3 = medium complexity core • 4 = low complexity core • 255 = invalid
number of modules	Number of modules on the VFC. Maximum number is 16.
number of voice devices (DSP)s	Number of possible DSPs. Maximum number is 96.
chans per vdevice	Number of channels (meaning calls) that each DSP can handle.
tot chans	Total number of channels.
tot active calls	Total number of active calls on this VFC.
module presense bit map	Indicates a 16-bit bitmap, each bit representing a module.

Field	Description
tdm mode	Time-division-multiplex bus mode. Values are as follows: • 0 = VFC is in classic mode. • 1 = VFC is in plus mode. This field should always be 1.
num_of_tdm_timeslots	Total number of calls that can be handled by the VFC.
auto recovery	Whether auto recovery is enabled. When autorecovery is enabled, the VRM tries to recover a DSP by resetting it if, for some reason, the DSP stops responding.
number of default voice file (core type images)	Number of DSPware files in use.
number of default voice file (maj ver)	Major version of the DSPware in use.
min ver	Minor version of the DSPware in use.
core_type	Type of DSPware in use. Values are as follows: • 1 = boot loader • 2 = high complexity core • 3 = medium complexity core • 4 = low complexity core
trough size	Indirect representation of the complexity of the DSPware in use. **Note** Effective with Cisco IOS Release 12.1(5)XM, this value is no longer displayed.
slop value	Indirect representation of the complexity of the DSPware in use. **Note** Effective with Cisco IOS Release 12.1(5)XM, this value is no longer displayed.

Field	Description
built-in codec bitmap	Bitmap of the codec built into the DSP firmware. Values are as follows: • CC_CAP_CODEC_G711U: 0x0001 • CC_CAP_CODEC_G711A: 0x0002 • CC_CAP_CODEC_G729IETF: 0x0004 • CC_CAP_CODEC_G729a: 0x0008 • CC_CAP_CODEC_G726r16: 0x0010 • CC_CAP_CODEC_G726r24: 0x0020 • CC_CAP_CODEC_G726r32: 0x0040 • CC_CAP_CODEC_G728: 0x0080 • CC_CAP_CODEC_G723r63: 0x0100 • CC_CAP_CODEC_G723r53: 0x0200 • CC_CAP_CODEC_GSM: 0x0400 • CC_CAP_CODEC_G729b: 0x0800 • CC_CAP_CODEC_G729ab: 0x1000 • CC_CAP_CODEC_G723ar63: 0x2000 • CC_CAP_CODEC_G723ar53: 0x4000 • CC_CAP_CODEC_G729: 0x8000 • CC_CAP_CODEC_GSMEFR: 0x40000 • CC_CAP_CODEC_T38FAX: 0x10000

Field	Description
loadable codec bitmap	Loadable codec bitmap for the loadable codecs. Values are as follows: • CC_CAP_CODEC_G711U: 0x0001 • CC_CAP_CODEC_G711A: 0x0002 • CC_CAP_CODEC_G729IETF: 0x0004 • CC_CAP_CODEC_G729a: 0x0008 • CC_CAP_CODEC_G726r16: 0x0010 • CC_CAP_CODEC_G726r24: 0x0020 • CC_CAP_CODEC_G726r32: 0x0040 • CC_CAP_CODEC_G728: 0x0080 • CC_CAP_CODEC_G723r63: 0x0100 • CC_CAP_CODEC_G723r53: 0x0200 • CC_CAP_CODEC_GSM: 0x0400 • CC_CAP_CODEC_G729b: 0x0800 • CC_CAP_CODEC_G729: = 0x1000 • CC_CAP_CODEC_G723ar63: 0x2000 • CC_CAP_CODEC_G723ar53: 0x4000 • CC_CAP_CODEC_G729: 0x8000 • CC_CAP_CODEC_GSMEFR: 0x40000 • CC_CAP_CODEC_T38FAX: 0x10000
fax codec bitmap	Fax codec bitmap. Values are as follows: • FAX_NONE = 0x1 • FAX_VOICE = 0x2 • FAX_144 = 0x80 • FAX_120 = 0x40 • FAX_96 = 0x20 • FAX_72 = 0x10 • FAX_48 = 0x08 • FAX_24 = 0x04
Logical Device (Tag)	Tag number or DSP number on the VFC.
Module#	Number identifying the module associated with a specific logical device.

Field	Description
DSP#	Number identifying the DSP on the VFC.
C_Ac	Number of active calls on the identified DSP.
C_Busy	Number of busied-out channels associated with the identified DSP.
C_Rst	Number of channels in the reset state associated with the identified DSP.
C_Bad	Number of defective ("bad") channels associated with the identified DSP.
Total active call channels	Total number of active calls.
Total busied out channels	Total number of busied-out channels.
Total channels in reset	Total number of channels in the reset state.
Total bad channels	Total number of defective channels.

Related Commands

Command	Description
show vrm active_calls	Displays active-only voice calls either for a specific VFC or for all VFCs.

show vsp

To display cumulative information about voice streaming processing (VSP) sessions, use the **show vsp** command in privileged EXEC mode.

show vsp {**all** | **debug** | **session** | **statistics**}

Syntax Description

all	Displays all available information on VSP sessions, including the information specified by the other keywords listed in this table.
debug	Displays the type of debugging information that is enabled by using the **debug vsp** command.
session	Displays cumulative statistics about active VSP sessions.
statistics	Displays statistics about active VSP sessions, including memory statistics.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.2(11)T	This command was introduced on the Cisco 3640, Cisco 3660, Cisco AS5300, Cisco AS5350, and Cisco AS5400.

Usage Guidelines

Use the **clear vsp statistics** command to reset the counters to 0 for the **show vsp** command.

Examples

The following is sample output from the **show vsp debug** command:

```
Router# show vsp debug
         VSP:<1>[0x62291660](0x62291660) debug_flag=0x7FF
```

The following is sample output from the **show vsp session** command:

```
Router# show vsp session
VSP_STATS:Session Statistics -
        sessions total=0; max_active=0, current=0
        session_duration last=0; max=0, min=0 ms
        pre_stream_wait last=0; max=0, min=0 ms
        stream_duration last=0; max=0, min=0 ms
        post_stream_wait last=0; max=0, min=0 ms
        stream_size last=0; max=0, min=0 bytes
        streaming_rate last=0; max=0, min=0 bytes/sec
        total_packet_count last=0; max=0, min=0 packets
        drop_packet_count last=0; max=0, min=0 packets
        particle_packet_count last=0; max=0, min=0 packets
```

The following is sample output from the **show vsp statistics** command:

```
Router# show vsp statistics
VSP_STATS:Session Statistics -
        sessions total=0; max_active=0, current=0
        session_duration last=0; max=0, min=0 ms
```

```
        pre_stream_wait last=0; max=0, min=0 ms
        stream_duration last=0; max=0, min=0 ms
        post_stream_wait last=0; max=0, min=0 ms
        stream_size last=0; max=0, min=0 bytes
        streaming_rate last=0; max=0, min=0 bytes/sec
        total_packet_count last=0; max=0, min=0 packets
        drop_packet_count last=0; max=0, min=0 packets
        particle_packet_count last=0; max=0, min=0 packets
VSP_STATS: Format Statistics -
        au_format_count=20
        wav_format_count=3
        other_format_count=0
VSP_STATS: Codec Statistics -
        codec_g729_count=4
        codec_g726_count=10
        codec_g711_count=0
        codec_g728_count=2
        codec_g723_count=5
        codec_gsm_count=2
        codec_other_count=0
VSP_STATS: Media Statistics -
        ram_count=23
        http_count=0
        smtp_count=0
        rtsp_count=0
        other_count=0
VSP_STATS:RTP Statistics -
        ts_gap_samples max=76800, min=80 samples
        [Unexpected SSRC Change (USC)]
                usc_count last=0; total=0, max=0, min=0
        [Out of sequence packet (OOSP)]
                oosp_count last=0; total=0, max=0, min=0
        [Unexpected timestamp gap (UTG)]
                max_utg_count last=0; total=0, max=0, min=0
        [Comfort Noise (CN)]
                max_cn_count last=4; total=70, max=8, min=4
        [Unexpected payload type or size (UPTS)]
                upt_count last=0; total=0, max=0, min=0; last_type=0
                ups_count last=0; total=198, max=61, min=0; last_size=2 bytes
        [Data exceeds limit (DEL)]
                del_count last=0; total=2, max=1, min=0
        [Silence exceeds timeout (SET)]
                set_count last=0; total=0, max=0, min=0
VSP_STATS:Packet Statistics -
        [Silence patching total (SPT)]
                spt_count last=296; total=7230, max=889, min=290
        [Concealment patching total (CPT)]
                cpt_count last=0; total=34, max=18, min=0
        [Normal patching total (NPT)]
                npt_count last=171; total=4249, max=453, min=106
```

The table below describes the fields shown in this output.

Table 220: show vsp statistics Field Descriptions

Field	Description
Session Statistics	Total number of VSP sessions since router startup or since the **clear vsp statistics** command was used. The active value should always be 0.
sessions total; max_active, current	

Field	Description
session_duration last; max, min	Duration of the last (most recent) session, and of the longest and shortest sessions in msecs.
pre_stream_wait last; max, min	Msecs that elapsed before the arrival of the first packet. Values are shown for last session, and for the session with the longest and shortest waits.
stream_duration last; max, min	Msecs between first packet arrival and last packet flush. Values are shown for last session, and for the session with the longest and shortest durations.
post_stream_wait last; max, min	Msecs between last packet flush and close of session.
stream_size last; max, min	Data streaming size.
streaming_rate last; max, min	Data streaming rate.
total_packet_count last; max, min	Total packets processed.
drop_packet_count last; max, min	Total packets dropped. The difference between the total packet count and packets dropped is the number of packets that have been accepted.
particle_packet_count last; max, min	Total particle packets processed.
Format Statistics	
au_format_count	Number of VSP sessions that used audio files in .au format.
wav_format_count	Number of VSP sessions that used audio files in .wav format.
other_format_count	Number of VSP sessions that used audio files of an unknown format.
Codec Statistics	
codec_g729_count	Number of VSP sessions that used the G.729 codec.
codec_g726_count	Number of VSP sessions that used the G.726 codec.
codec_g711_count	Number of VSP sessions that used the G.711 codec.
codec_g728_count	Number of VSP sessions that used the G.728 codec.
codec_g723_count	Number of VSP sessions that used the G.723 codec.
codec_gsm_count	Number of VSP sessions that used the GSM codec.
codec_other_count	Number of VSP sessions that used an unknown codec.
Media Statistics	
ram_count	Total number of RAM recordings and playouts.

Field	Description
http_count	Total number of HTTP recordings and playouts.
smtp_count	Total number of SMTP recordings.
rtsp_count	Total number of RTSP recordings and playouts.
other_count	Should always be 0.
RTP Statistics	
ts_gap_samples max min	Permissible timestamp gap in samples.
[Unexpected SSRC Change (USC)]	
usc_count last; total, max, min	Number of times that the source of the streaming has changed.
[Out of sequence packet (OOSP)]	
oosp_count last; total, max, min	Number of out-of-sequence packets.
[Unexpected timestamp gap (UTG)]	
max_utg_count last; total, max, min	Number of packets with an unexpected timestamp gap.
[Unexpected payload type or size (UPTS)]	
upt_count last; total, max, min; last_type	Number of comfort noise packets.
ups_count last; total, max, min; last_size	Number of packets with unexpected nonvoice payload sizes.
[Data exceeds limit (DEL)]	
del_count last; total, max, min	Number of times that the total recording size is larger than the preset recording size.
[Silence exceeds timeout (SET)]	
set_count last; total, max, min	Number of times that the timestamp gap is larger than the preset timeout value.
Packet Statistics	
[Silence patching total (SPT)]	
spt_count last; total, max, min	Number of silence packets that have been inserted during recording.
[Concealment patching total (CPT)]	
cpt_count last; total, max, min	Number of concealment packets that have been inserted during recording.
[Normal patching total (NPT)]	

Field	Description
npt_count last; total, max, min	Number of normal packets that have been patched during recording.

Related Commands

Command	Description
clear vsp statistics	Clears the statistics for VSP sessions.

show wsapi

To display information on the Cisco Unified Communication IOS services, including registration, statistics, and route information, use the **show wsapi** command in user EXEC or privileged EXEC mode.

show wsapi {**http-client** | **http-server** | **registration** | **registration** {**all** | **xcc** | **xcdr** | **xsvc**} | **svcc route**}

Syntax Description

http-client	Displays the statistics that have been collected on the http client interface.
http-server	Displays the statistics that have been collected on the http server interface.
registration	Displays the currently registered applications on the WSAPI subsystem.
all	Displays all registered applications.
xcc	Displays the applications that are registered to the XCC provider.
xcdr	Displays the applications that are registered to the XCDR provider.
xsvc	Displays the applications that are registered to the XSVC provider.
xsvc route	Displays the internal route information in the XSVC provider.

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
15.2(2)T	This command was introduced.

Usage Guidelines

Use this command to display information on the Cisco Unified Communication IOS services.

Examples

The following example shows a sample output from the **show wsapi http-client** command.

```
Router# show wsapi http-client

WSAPI Outgoing Notify/Solicit Message Statistics
========================================
wsapi_show_httpc_callback_context_invalid: 0
wsapi_show_httpc_callback_context_error: 0
wsapi_show_httpc_callback_no_reg: 5
wsapi_show_httpc_callback_notify_OK: 85
wsapi_show_httpc_callback_notify_error: 0
wsapi_show_httpc_callback_client_error: 0
wsapi_show_httpc_callback_error: 7
wsapi_show_httpc_callback_client_error: 0
wsapi_show_httpc_callback_decode_error: 28
wsapi_show_httpc_callback_no_txID: 0
wsapi_show_httpc_callback_OK: 655
wsapi_show_httpc_create_msg_error: 0
```

```
wsapi_show_httpc_context_active: 0
wsapi_tx_context_freeq depth: 4
```

The following example shows a sample output from the **show wsapi http-server** command.

```
Router# show wsapi http-server

WSAPI Incoming Request Message Statistics
=========================================
wsapi_show_https_urlhook: 23
wsapi_show_https_post_action: 23
wsapi_show_https_post_action_fail: 0
wsapi_show_https_xml_fault: 0
wsapi_show_https_post_action_done: 23
wsapi_show_https_service_timeout: 0
wsapi_show_https_send_error: 0
wsapi_show_https_invalid_context: 0
wsapi_show_https_data_active: 0
wsapi_https_data_q depth: 1
wsapi_show_https_internal_service_error: 0
wsapi_show_https_service_unavailable_503: 0
wsapi_show_https_not_found_404: 0
wsapi_show_https_registration_success: 9
wsapi_show_https_not_registered: 0
wsapi_show_https_registration_auth_fail: 1
wsapi_show_https_registration_fail: 0
wsapi_show_https_un_registered: 0
```

The following example shows a sample output from the **show wsapi registration** command.

```
Router# show wsapi registration

Provider XCC
=====================================================
registration
id: 4FA11CC:XCC:myapp:5
appUrl:http://sj22lab-as2:8090/xcc
appName: myapp
provUrl: http://10.1.1.1:8090/cisco_xcc
prober state: STEADY
connEventsFilter:
CREATED|AUTHORIZE_CALL|ADDRESS_ANALYZE|REDIRECTED|ALERTING|CONNECTED|TRANSFERRED|CALL_DELIVERY|DISCONNECTED|HANDOFF_JOIN|HANDOFF_LEAVE
mediaEventsFilter:
DTMF|MEDIA_ACTIVITY|MODE_CHANGE||TONE_DIAL|TONE_OUT_OF_SERVICE|TONE_RINGBACK|TONE_SECOND_DIAL
blockingEventTimeoutSec: 1
blockingTimeoutHandle: CONTINUE_PROCESSING

Provider XSVC
=====================================================
registration index: 2
id: 4FA0F8C:XSVC:myapp:3
appUrl:http://sj22lab-as2:8090/xsvc
appName: myapp
provUrl: http://10.1.1.1:8090/cisco_xsvc
prober state: STEADY
route filter:
event filter: off

Provider XCDR
=====================================================
registration index: 1
id: 4FA10A0:XCDR:myapp:1
appUrl:http://sj22lab-as2:8090/xcdr
```

```
appName: myapp
provUrl: http://10.1.1.1:8090/cisco_xcdr
prober state: STEADY
cdr format: COMPACT
event filter: off
```

The following example shows a sample output from the **show wsapi xsvc route** command.

```
Router# show wsapi xsvc route

Route SANJOSE_SIP
=================================================
Type: VOIP
Description: OUT
Filter:
Trunk:
Trunk Name: 1.3.45.2
Trunk Type: SIPV2
Trunk Status: UP
Route SANJOSE_PRI
=================================================
Type: PSTN
Description: IN
Filter:
Trunk:
Trunk Name: Se0/1/0:23
Trunk Type: ISDN PRI
Trunk Status: UP
Total channels 2
Channel bitmap 0x01FFFFFE 1-24
Link bitmap 0x00000006
Alarm 0x00000001
Time elapsed 516
Interval 92
CurrentData
0 Line Code Violations, 0 Path Code Violations
0 Slip Secs, 0 Fr Loss Secs, 0 Line Err Secs, 0 Degraded Mins
0 Errored Secs, 0 Bursty Err Secs, 0 Severely Err Secs, 0 Unavail Secs
TotalData
49 Line Code Violations, 7 Path Code Violations,
0 Slip Secs, 1 Fr Loss Secs, 1 Line Err Secs, 0 Degraded Mins,
0 Errored Secs, 0 Bursty Err Secs, 0 Severely Err Secs, 2 Unavail Secs
Trunk Name: Se0/1/1:23
Trunk Type: ISDN PRI
Trunk Status: UP
Total channels 2
Channel bitmap 0x01FFFFFE 1-24
Link bitmap 0x00000006
Alarm 0x00000001
Time elapsed 516
Interval 92
CurrentData
0 Line Code Violations, 0 Path Code Violations
0 Slip Secs, 0 Fr Loss Secs, 0 Line Err Secs, 0 Degraded Mins
0 Errored Secs, 0 Bursty Err Secs, 0 Severely Err Secs, 0 Unavail Secs
TotalData
42 Line Code Violations, 4 Path Code Violations,
0 Slip Secs, 1 Fr Loss Secs, 1 Line Err Secs, 0 Degraded Mins,
0 Errored Secs, 0 Bursty Err Secs, 0 Severely Err Secs, 2 Unavail Secs
```

Related Commands

Command	Description
provider	Enables a Cisco Unified Communicatoins IOS service provider.

show xcsp port

To display the status of a router port under the control of the external control service provider (XCSP) sub**sy**stem, use the **show xcsp port**command in privileged EXEC mode.

show xcsp port *slot-num port-num*

Syntax Description

slot -num	Slot number of the interface card. Values are as follows: • Cisco AS5350: From 0 to 3. • Cisco AS5400: From 0 to 7. • Cisco AS5850: From 0 to 5 and from 8 to 13. Slots 6 and 7 are reserved for the route switch controller (RSC).
port -num	Port number of the interface card. Values are as follows: • Cisco AS5350: For T1/E1, from 0 to 7. For T3, from 1 to 28. • Cisco AS5400: For T1/E1, from 0 to 7. For T3, from 1 to 28. • Cisco AS5850: For T1/E1, from 0 to 23. For T3, from 1 to 28.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(2)XB	This command was introduced.
12.2(11)T	The command was integrated into Cisco IOS Release 12.2(11)T and implemented on the Cisco AS5850.

Examples

The following is sample output from this command:

```
Router# show xcsp port 1 0
Slot 1 configured
Number of ports configured=1 slot state= Up
================================================
Port 0 State= Up type = 5850 24 port T1
Channel states
  0  Idle
  1  Idle
  2  Idle
  3  Idle
  4  Idle
  .
  .
  .
  22  Idle
  23  Idle
```

The table below describes significant fields in this output.

Note To get the field description output, you must enter the *slot-num* and *port-num* arguments for the **show xcsp port** command.

Table 221: show xcsp port Field Descriptions

Field	Descriptions
Port	Port number. Range is from 1 to 28.
State	Port state; can be Up or Down.
type	T1 or E1 ports on the AS5400: 8. T1 or E1 ports on the AS5850: 24. T3 ports on the AS5400 and AS5850: 28.
Channel states	Channel states. Values are as follows: • Blocked • Connection in progress • Cot Check In Progress • Cot Check Pending • Down • Idle • In Release in progress • In Use • Invalid • Loopback • Not Present • Out of Service • Out Release in progress • Playing Tone • Shutdown

Related Commands

Command	Description
show xcsp slot	Displays the status of XCSP slots.

show xcsp slot

To display the status of a router slot under the control of the external control service provider (XCSP) subsystem, use the **show xcsp slot** command in privileged EXEC mode.

show xcsp slot *slot-num*

Syntax Description

slot -num	The slot number of the T1 or E1 interface card. Values are as follows: • Cisco AS5350: From 0 to 3. • Cisco AS5400: From 1 to 7. • Cisco AS5850: From 0 to 5 and from 8 to 13. Slots 6 and 7 are reserved for the route switch controller (RSC).

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(2)XB	This command was introduced.
12.2(11)T	The command was integrated into Cisco IOS Release 12.2(11)T and implemented on the Cisco AS5850.

Examples

The following is sample output from this command:

```
Router# show xcsp slot 1
Slot 1 configured
Number of ports configured=1 slot state= Up
```

The table below describes significant fields shown in this output.

Table 222: show xcsp slot Field Descriptions

Field	Description
slot state	Slot state; can be either Up or Down.

Related Commands

Command	Description
show xcsp port	Displays the status of XCSP ports.

shut

To shut down a set of digital signal processors (DSPs) on the Cisco 7200 series router, use the **shut** command in DSP configuration mode. To put DSPs back in service, use the **no** form of this command.

shut *number*
no shut *number*

Syntax Description

number	Number of DSPs to be shut down.

Command Default

No shut

Command Modes

DSP configuration

Command History

Release	Modification
12.0(5)XE	This command was introduced on the Cisco 7200 series.
12.1(1)T	This command was modified to add information about DSP groups.

Usage Guidelines

This command applies to VoIP on the Cisco 7200 series routers.

Examples

The following example shuts down two sets of DSPs:

```
shut 2
```

shutdown (Annex G neighbor)

To disable the service relationships requirement for border elements, use the **shutdown** command in config-nxg-neigh-srvc mode. To enable the service relationship for border elements, use the **no**form of this command.

shutdown
no shutdown

Syntax Description

This command has no arguments or keywords.

Command Default

The Annex G neighbor is shut down.

Command Modes

Annex G neighbor service (config-nxg-neigh-svc)

Command History

Release	Modification
12.2(11)T	This command was introduced.

Usage Guidelines

The **no shutdown** command verifies that a domain name has been configured and ensures that the border element has been configured to reject messages from unknown "stranger" border elements.

Examples

The following example enables the border element:

```
Router(config-nxg-neigh-srvc)# no shutdown
```

Related Commands

Command	Description
access -policy	Requires that a neighbor be explicitly configured.
inbound ttl	Sets the inbound time-to-live value.
outbound retry -interval	Defines the retry period for attempting to establish the outbound relationship between border elements.
retry interval	Defines the time between delivery attempts.
retry window	Defines the total time that a border element attempts delivery.

shutdown (Annex G)

To shut down the Annex G border element (BE), use the **shutdown** command in Annex G configuration mode. To reinstate the Annex G BE, use the no form of this command.

shutdown
no shutdown

Syntax Description

This command has no arguments or keywords.

Command Default

The Annex G border element is not shut down.

Command Modes

Annex G configuration (config-annexg)

Command History

Release	Modification
12.2(2)XA	This command was introduced.
12.2(4)T	This command was integrated into Cisco IOS Release 12.2(4)T. This command was not supported on the Cisco AS5300, Cisco AS5350, and Cisco AS5400 in this release.
12.2(2)XB1	This command was implemented on the Cisco AS5850.
12.2(11)T	This command was integrated into Cisco IOS Release 12.2(11)T.

Usage Guidelines

While the Annex G BE is in shutdown state, all Annex G messages received from neighbors are ignored and the colocated gatekeeper does not use the Annex G BE for address resolution.

Examples

The following example shuts the BE down:

```
Router(config)# call-router h323-annexg be20
Router(config-annexg)# shutdown
```

Related Commands

Command	Description
call -router	Enables the Annex G border element configuration commands.
show call -router status	Displays the Annex G BE status.

shutdown (dial-peer)

To change the administrative state of the selected dial peer from up to down, use the **shutdown** command in dial-peer configuration mode. To change the administrative state of this dial peer from down to up, use the **no** form of this command.

shutdown
no shutdown

Syntax Description

This command has no arguments or keywords.

Command Default

No shutdown

Command Modes

Dial-peer configuration (config-dial-peer)

Command History

Release	Modification
11.3(1)T	This command was introduced on the Cisco 3600 series.
12.1(1)	This command was modified for store-and-forward fax.

Usage Guidelines

When a dial peer is shut down, you cannot initiate calls to that peer.

This command applies to both on-ramp and off-ramp store-and-forward fax functions.

Examples

The following example changes the administrative state of voice telephony (plain old telephone service [POTS]) dial peer 10 to down:

```
dial-peer voice 10 pots
shutdown
```

The following example changes the administrative state of voice telephony (POTS) dial peer 10 to up:

```
dial-peer voice 10 pots
no shutdown
```

Related Commands

Command	Description
dial -peer voice	Enters dial-peer configuration mode, defines the type of dial peer, and defines the dial-peer tag number.

shutdown (DSP Farm profile)

To disable the digital signal processor (DSP) farm profile, use the **shutdown** command in DSP farm profile configuration mode. To allocate DSP farm resources and associate with the application, use the **no** form of this command.

shutdown
no shutdown

Syntax Description

This command has no arguments or keywords.

Command Default

Disabled

Command Modes

DSP farm profile configuration (config-dspfarm-profile)

Command History

Release	Modification
12.3(8)T	This command was introduced.

Usage Guidelines

It is essential that the profile be disabled by using the **shutdown** command before a DSP farm profile is updated.

Examples

The following example allocates DSP farm resources and associates with the application:

```
Router(config-dspfarm-profile)#
 no shutdown
```

Related Commands

Command	Description
codec (dspfarm-profile)	Specifies the codecs supported by a DSP farm profile.
description (dspfarm-profile)	Includes a specific description about the DSP farm profile.
dspfarm profile	Enters the DSP farm profile configuration mode and defines a profile for DSP farm services.
maximum sessions (dspfarm-profile)	Specifies the maximum number of sessions that need to be supported by the profile.

shutdown (gatekeeper)

To disable the gatekeeper, use the **shutdown** command in gatekeeper configuration mode. To enable the gatekeeper, use the **no** form of this command.

shutdown
no shutdown

Syntax Description

This command has no arguments or keywords.

Command Default

Disabled (shut down)

Command Modes

Gatekeeper configuration (config-gk)

Command History

Release	Modification
11.3(2)NA	This command was introduced on the Cisco 2500 series and Cisco 3600 series.
12.0(3)T	The command was integrated into Cisco IOS Release 12.0(3)T and implemented on the Cisco MC3810.

Usage Guidelines

The gatekeeper does not have to be enabled before you can use the other gatekeeper configuration commands. In fact, it is recommended that you complete the gatekeeper configuration before bringing up the gatekeeper because some characteristics may be difficult to alter while the gatekeeper is running, as there may be active registrations or calls.

The no shutdown command enables the gatekeeper, but it does not make the gatekeeper operational. The two exceptions to this are as follows:

- If no local zones are configured, a **no shutdown** command places the gatekeeper in INACTIVE mode waiting for a local zone definition.
- If local zones are defined to use an HSRP virtual address, and the HSRP interface is in STANDBY mode, the gatekeeper goes into HSRP STANDBY mode. Only when the HSRP interface is ACTIVE does the gatekeeper go into the operational UP mode.

Examples

The following command disables a gatekeeper:

```
shutdown
```

Related Commands

Command	Description
shutdown (gateway)	Shuts down all VoIP call service on a gateway.

shutdown (gateway)

To shut down all VoIP call service on a gateway, use the **shutdown**commandin voice service configuration mode. To enable VoIP call service, use the **no** form of this command.

shutdown [**forced**]
no shutdown

Syntax Description

forced	(Optional) Forces the gateway to immediately terminate all in-progress calls.

Command Default

Call service is enabled

Command Modes

Voice service configuration (config-voi-serv)

Command History

Release	Modification
12.3(1)	This command was introduced.
Cisco IOS XE Amsterdam 17.2.1r	Introduced support for YANG models.

Examples

The following example shows VoIP call service being shut down on a Cisco gateway:

```
voice service voip
shutdown
```

The following example shows VoIP call service being enabled on a Cisco gateway:

```
voice service voip
no shutdown
```

Related Commands

Command	Description
shutdown (gatekeeper)	Disables the gatekeeper.

shutdown (mediacard)

To disable a selected media card, use the **shutdown** command in mediacard configuration mode. To enable a selected media card, use the **no** form of this command.

shutdown
no shutdown

Syntax Description

This command has no arguments or keywords.

Command Default

No default behavior or values

Command Modes

Media card configuration

Command History

Release	Modification
12.3(8)XY	This command was introduced on the Communication Media Module.
12.3(14)T	This command was integrated into Cisco IOS Release 12.3(14)T.
12.4(3)	This command was integrated into Cisco IOS Release 12.4(3).

Usage Guidelines

Use the **no shutdown** command at the end of media card configuration. If there are any active connections when you disable the media card, the Digital Signal Processor Resource Manager (DSPRM) displays a warning message indicating that the DSP resources allocated on other media cards for some of the resource pool in this media card will be removed or that there are active connections available in this resource pool and prompts you for a response. Profiles that use resources on this card must be brought up separately after using this command.

Examples

The following example shows how to enable a media card:

```
no shutdown
```

Related Commands

Command	Description
resource-pool	Creates a DSP resource pool on the selected media card.

shutdown (auto-config application)

To disable an auto-configuration application for download, use the **shutdown** command in auto-config application configuration mode. To enable an auto-configuration application for download, use the **no**form of this command.

shutdown
no shutdown

Syntax Description

This command has no keywords or arguments.

Command Default

Disabled

Command Modes

Auto-config application configuration (auto-config-app)

Command History

Release	Modification
12.3(8)XY	This command was introduced on the Communication Media Module.
12.3(14)T	This command was integrated into Cisco IOS Release 12.3(14)T.

Examples

The following example shows the **shutdown** command used to enable an auto-configuration application for download:

```
Router(auto-config-app)# no shutdown
```

Related Commands

Command	Description
auto-config	Enables auto-configuration or enters auto-config application configuration mode for the SCCP application.
show auto-config	Displays the current status of auto-configuration applications.

shutdown (RLM)

To shut down all of the links under the RLM group, use the **shutdown** command in RLM configuration mode. RLM does not try to reestablish those links until the command is negated. To disable this function, use the **no** form of this command.

shutdown
no shutdown

Syntax Description

This command has no arguments or keywords.

Command Default

Disabled

Command Modes

RLM configuration

Command History

Release	Modification
11.3(7)	This command was introduced.

Related Commands

Command	Description
clear interface	Resets the hardware logic on an interface.
clear rlm group	Clears all RLM group time stamps to zero.
interface	Defines the IP addresses of the server, configures an interface type, and enters interface configuration mode.
link (RLM)	Specifies the link preference.
protocol rlm port	Reconfigures the port number for the basic RLM connection for the whole rlm-group.
retry keepalive	Allows consecutive keepalive failures a certain amount of time before the link is declared down.
server (RLM)	Defines the IP addresses of the server.
show rlm group statistics	Displays the network latency of the RLM group.
show rlm group status	Displays the status of the RLM group.
show rlm group timer	Displays the current RLM group timer values.
timer	Overwrites the default setting of timeout values.

shutdown (settlement)

To deactivate the settlement provider, use the shutdown command in settlement configuration mode. To activate a settlement provider, use the no **shutdown** command.

shutdown
no shutdown

Syntax Description

This command has no arguments or keywords.

Command Default

The default status of a settlement provider is deactivated. The settlement provider is down.

Command Modes

Settlement configuration

Command History

Release	Modification
12.0(4)XH1	This command was introduced on the Cisco 2500 series, Cisco 3600 series, and Cisco AS5300.
12.1(1)T	This command was integrated into Cisco IOS Release 12.1(1)T.

Usage Guidelines

Use this command at the end of the configuration of a settlement server to bring up the provider. This command activates the provider. Otherwise, transactions do not go through the provider to be audited and charged. Use the shutdown command to deactivate the provider.

Examples

The following example enables a settlement server:

```
settlement 0
 no shutdown
```

The following example disables a settlement server:

```
settlement 0
 shutdown
```

Related Commands

Command	Description
connection -timeout	Configures the time that a connection is maintained after completing a communication exchange.
customer -id	Identifies a carrier or ISP with a settlement provider.
device -id	Specifies a gateway associated with a settlement provider.
encryption	Sets the encryption method to be negotiated with the provider.
max -connection	Sets the maximum number of simultaneous connections to be used for communication with a settlement provider.
response -timeout	Configures the maximum time to wait for a response from a server.

Command	Description
retry -delay	Sets the time between attempts to connect with the settlement provider.
session -timeout	Sets the interval for closing the connection when there is no input or output traffic.
settlement	Enters settlement configuration mode and specifies the attributes specific to a settlement provider.
type	Configures an SAA-RTR operation type.

shutdown (trace)

To disable the VoIP Trace framework in CUBE, use the **shutdown** command in trace configuration mode. To re-enable VoIP tracing, use the **no** form of this command.

Syntax Description

shutdown	Disables the VoIP Trace framework.
[no] shutdown	Enables the VoIP Trace framework.

Command Default

VoIP Trace is enabled by default.

Command Modes

Trace configuration mode (conf-serv-trace)

Command History

Release	Modification
Cisco IOS XE Amsterdam 17.3.2 Cisco IOS XE Bengaluru 17.4.1a	This command was introduced for Cisco Unified Border Element.

Usage Guidelines

VoIP Trace is disabled using the command **shutdown** under the **trace** configuration mode as follows:

```
router (config)#voice service voip
router(conf-voi-serv)#trace
router(conf-serv-trace)#?
Voip Trace submode commands:
default      Set a command to its defaults
exit         Exit from voice service voip trace mode
no           Negate a command or set its defaults
shutdown     Shut Voip Trace debugging
memory-limit Set limit based on memory used
router(conf-serv-trace)#shutdown
```

To re-enable VoIP Trace, configure the CLI command **no shutdown** under the **trace** configuration mode as follows:

```
router (config)#voice service voip
router(conf-voi-serv)#trace
router(conf-serv-trace)#no ?
exit     Exit from voice service voip trace mode
shutdown Shut Voip Trace debugging
router(conf-serv-trace)# no shutdown
```

If you configure **shutdown** :

- Tracing for active calls is stopped.
- All existing traces in memory are deleted.

Only new calls received after VoIP Trace is enabled are monitored.

Examples

The following is a sample of CLI command **shutdown** configured under trace configuration sub-mode:

```
router (config)#voice service voip
router(conf-voi-serv)#trace
router(conf-serv-trace)#shutdown
```

Related Commands

Command	Description
memory-limit (trace)	Defines the memory limit for storing VoIP Trace information.
trace	Enables the VoIP Trace serviceability framework in CUBE.
show voip trace	Displays the VoIP Trace information for SIP legs on a call received on CUBE

shutdown (voice-port)

To take the voice ports for a specific voice interface card offline, use the **shutdown** command in voice-port configuration mode. To put the ports back in service, use the **no** form of this command.

shutdown
no shutdown

Syntax Description

This command has no arguments or keywords.

Command Default

Shutdown

Command Modes

Voice-port configuration (config-voiceport)

Command History

Release	Modification
11.3(1)T	This command was introduced on the Cisco 3600 series.
12.4(22)T	Support for IPv6 was added.

Usage Guidelines

When you use this command, all ports on the voice interface card are disabled. When you use the **no**form of the command, all ports on the voice interface card become enabled. A telephone connected to an interface hears silence when a port is shut down.

Examples

The following example takes voice port 1/1/0 offline:

```
voice-port 1/1/0
shutdown
```

Related Commands

Command	Description
shutdown (port)	Disables a port.



signal through srv version

- signal, on page 1101
- signal did, on page 1105
- signal keepalive, on page 1106
- signal pattern, on page 1108
- signal sequence oos, on page 1111
- signal timing idle suppress-voice, on page 1113
- signal timing oos, on page 1116
- signal timing oos restart, on page 1118
- signal timing oos standby, on page 1120
- signal timing oos suppress-all, on page 1122
- signal timing oos suppress-voice, on page 1124
- signal timing oos timeout, on page 1126
- signaling forward, on page 1128
- signaling forward (dial peer), on page 1133
- signal-type, on page 1138
- silent-discard untrusted, on page 1140
- silent-fax, on page 1141
- sip, on page 1142
- sip-header, on page 1144
- sip-header SIP-StatusLine, on page 1145
- sip-server, on page 1146
- sip-ua, on page 1148
- sni send (voice class), on page 1151
- snmp enable peer-trap dscp-profile, on page 1152
- snmp enable peer-trap poor-qov, on page 1153
- snmp-server enable traps voice (DSCP profile), on page 1154
- soft-offhook, on page 1155
- source-address (uc-wsapi), on page 1157
- source carrier-id, on page 1158
- source filter, on page 1159
- source-ip (media-profile), on page 1160
- source trunk-group-label, on page 1161
- speed dial, on page 1162

- srtp (dial peer), on page 1165
- srtp (voice), on page 1167
- srtp-auth, on page 1169
- srtp-crypto, on page 1171
- srtp negotiate, on page 1173
- srv version, on page 1175

signal

To specify the type of signaling for a voice port, use the **signal** command in voice-port configuration mode. To reset to the default, use the **no** form of this command.

Foreign Exchange Office (FXO) and Foreign Exchange Station (FXS) Voice Ports
signal {**groundstart** | **loopstart** [**live-feed**]}
no signal {**groundstart** | **loopstart**}

Ear and mouth (EandM) Voice Ports
signal {**delay-dial** | **immediate** | **lmr** | **wink-start**}
no signal {**delay-dial** | **immediate** | **lmr** | **wink-start**}

Centralized Automatic Message Accounting (CAMA) Ports
signal {**cama** {**kp-0-nxx-xxxx-st** | **kp-0-npa-nxx-xxxx-st** | **kp-2-st** | **kp-npd-nxx-xxxx-st** | **kp-0-npa-nxx-xxxx-st-kp-yyy-yyy-yyyy-st**} | **groundstart** | **loopstart**}
no signal {**cama** {**kp-0-nxx-xxxx-st** | **kp-0-npa-nxx-xxxx-st** | **kp-2-st** | **kp-npd-nxx-xxxx-st** | **kp-0-npa-nxx-xxxx-st-kp-yyy-yyy-yyyy-st**} | **groundstart** | **loopstart**}

Syntax Description

groundstart	Specifies the use of groundstart signaling. Used for FXO and FXS interfaces. Groundstart signaling allows both sides of a connection to place a call and to hang up. **Note** The CAMA version of this keyword is **groundstart**. Both forms operate identically.
loopstart	Specifies the use of loop start signaling. Used for FXO and FXS interfaces. With loopstart signaling, only one side of a connection can hang up. This is the default setting for FXO and FXS voice ports. **Note** The CAMA version of this keyword is **loopstart**. Both forms operate identically.
live-feed	(Optional) Enables an MOH audio stream from a live feed to be directly connected to the router through an FXO port.
delay-dial	The calling side seizes the line by going off-hook on its E-lead. After a timing interval, the calling side looks at the supervision from the called side. If the supervision is on-hook, the calling side starts sending information as dual tone multifrequency (DTMF) digits; otherwise, the calling side waits until the called side goes on-hook and then starts sending address information. Used for E&M tie trunk interfaces.
immediate	The calling side seizes the line by going off-hook on its E-lead and sends address information as DTMF digits. Used for E&M tie trunk interfaces.

lmr	Specifies the use of Land Mobile Radio signaling.
wink-start	The calling side seizes the line by going off-hook on its E-lead then waits for a short off-hook "wink" indication on its M-lead from the called side before sending address information as DTMF digits. Used for E&M tie trunk interfaces. This is the default setting for E&M voice ports.
cama	Selects and configures the port for 911 calls.
kp-0-npa-nxx-xxxx-st	10-digit transmission. The E.164 number is fully transmitted.
kp-0-npa-nxx-xxxx-st-kp-yyy-yyy-yyyy-st	Supports CAMA Signaling with ANI/Pseudo ANI (PANI).
kp-0-nxx-xxxx-st	7-digit automatic number identification (ANI) transmission. The Numbering Plan Area (NPA) or area code is implied by the trunk group and is not transmitted.
kp-2-st	Default transmission when the CAMA trunk cannot get a corresponding Numbering Plan Digit (NPD) digit in the lookup table, or when the calling number is fewer than ten digits in length. (NPA digits are not available.)
kp-npd-nxx-xxxx-st	8-digit ANI transmission, where the NPD is a single multifrequency (MF) digit that is expanded into the NPA. The NPD table is preprogrammed in the sending and receiving equipment (on each end of the MF trunk); for example: 0 = 415, 1 = 510, 2 = 650, 3 = 916 05550100 = (415) 555-0100, 15550100 = (510) 555-0100, and so on. NPD range is from 0 to 3.

Command Default

FXO and FXS interfaces: **loopstart** E&M interfaces: **wink-start** CAMA interfaces: **loopstart**

Command Modes

Voice-port configuration (config-voiceport)

Command History

Release	Modification
11.3(1)T	This command was introduced on the Cisco 3600 series.
12.2(11)T	This command was modified to support ANI transmission.
12.3(4)XD	The **lmr** keyword was added.
12.3(7)T	This command was integrated into Cisco IOS Release 12.3(7)T.
12.3(14)T	This command was implemented on the Cisco 2800 series and Cisco 3800 series.
12.4(9)T	The kp-0-npa-nxx-xxxx-st-kp-yyy-yyy-yyyy-st keyword was added to support CAMA Signaling with ANI/Pseudo ANI (PANI).
12.4(11)XJ	The **live-feed** keyword was added.

Release	Modification
12.4(15)T	The **live-feed** keyword was integrated into Cisco IOS Release 12.4(15)T.

Usage Guidelines

This command applies to analog voice ports only. A voice port must be shut down and then activated before the configured values take effect.

For an E&M voice port, this command changes only the signal value for the selected voice port.

For an FXO or FXS voice port, this command changes the signal value for both voice ports on a voice port module (VPM). If you change the signal type for an FXO voice port on Cisco 3600 series routers, you need to move the appropriate jumper in the voice interface card of the voice network module. For more information about the physical characteristics of the voice network module, see the installation documentation that came with your voice network module.

Some PBXs miss initial digits if the E&M voice port is configured for immediate start signaling. Immediate start signaling should be used for dial pulse outpulsing only and only on circuits for which the far end is configured to accept digits within a few milliseconds of seizure. Delay dial signaling, which is intended for use on trunks and not lines, relies on the far end to return an off-hook indication on its M-lead as soon as the circuit is seized. When a receiver is attached, the far end removes the off-hook indication to indicate that it is ready to receive digits. Delay dial must be configured on both ends to work properly. Some non-Cisco devices have a limited number of DTMF receivers. This type of equipment must delay the calling side until a DTMF receiver is available.

To specify which VIC-2CAMA ports are designated as dedicated CAMA ports for emergency 911 calls, use the **signal cama** command. No two service areas in the existing North American telephony infrastructure supporting E911 calls have identical service implementations, and many of the factors that drive the design of emergency call handling are matters of local policy and therefore outside the scope of this document. Local policy determines which ANI format is appropriate for the specified Physical Service Access Point (PSAP) location.

The following four types of ANI transmittal schemes are based on the actual number of digits transmitted toward the E911 tandem. In each instance, the actual calling number is proceeded with a key pulse (KP) followed by an information (I) field or a NPD, which is then followed by the ANI calling number, and finally is followed by a start pulse (ST), STP, ST2P, or ST3P, depending on the trunk group type in the PSTN and the traffic mix carried.

The information field is one or two digits, depending on how the circuit was ordered originally. For one-digit information fields, a value of 0 indicates that the calling number is available. A value of 1 indicates that the calling number is not available. A value of 2 indicates an ANI failure. For a complete list of values for two-digit information fields, see *SR-2275: Telcordia Notes on the Networks* at www.telcordia.com .

- 7-digit transmission (**kp 0 nxx xxxx st**):

The calling phone number is transmitted, and the NPA is implied by the trunk group and not transmitted.

- 8-digit transmission (**KP npd nxx xxxx st**) :

The I field consists of single-digit NPD-to-NPA mapping. When the calling party number of 415-555-0122 places a 911 call, and the Cisco 2600 series or Cisco 3600 series has an NPD (0)-to-NPA (415) mapping, the NPA signaling format is received by the selective router at the central office (CO).

Note NPD values greater than 3 are reserved for signifying error conditions.

- 10-digit transmission (**kp 0 npa nxx xxxx st)**

The E.164 number is fully transmitted.

- 20-digit transmission (**kp-0-npa-nxx-xxxx-st-kp-yyy-yyy-yyyy-st**):

Twenty digits support (two 10 digit numbers) on FGD-OS in the following format, KP+II+10 digit ANI+ST+KP+7/10 digit PANI+ ST

- kp-2-st transmission (**kp-2-st**):

kp-2-st transmission is used if the PBX is unable to out-pulse the ANI. If the ANI received by the Cisco router is not as per configured values, kp-2-st is transmitted. For example, if the voice port is configured for out-pulsing a ten-digit ANI and the 911 call it receives has a seven-digit calling party number, the router transmits kp-2-st.

Note Emergency 911 calls are not rejected for an ANI mismatch. The call establishes a voice path. The E911 network, however, does not receive the ANI.

Examples

The following example configures groundstart signaling on the Cisco 3600 series as the signaling type for a voice port, which means that both sides of a connection can place a call and hang up:

```
voice-port 1/1/1
 signal groundstart
```

The following example configures a ten-digit ANI transmission:

```
Router(config)#
voice-port 1/0/0
Router(config-voiceport)# signal cama kp-0-npa-nxx-xxxx-st
```

The following example configures 20-digit CAMA Signaling with ANI/Pseudo ANI:

```
Router(config-voiceport)# signal cama KP-0-NPA-NXX-XXXX-ST-KP-YYY-YYY-YYYY-ST
```

Related Commands

Command	Description
ani mapping	Preprograms the NPA, or area code, into a single MF digit.

signal did

To enable direct inward dialing (DID) on a voice port, use the **signal did command in**voice-port configuration mode. To disable DID and reset to loop-start signaling, use the **no** form of this command.

signal did { **immediate-start** | **wink-start** | **delay-dial** }
no signal did

Syntax Description

immediate -start	Enables immediate-start signaling on the DID voice port.
wink -start	Enables wink-start signaling on the DID voice port.
delay -start	Enables delay-dial signaling on the DID voice port.

Command Default

No default behavior or values

Command Modes

Voice-port configuration (config-voiceport)

Command History

Release	Modification
12.1(5)XM	This command was introduced on the Cisco 2600 series and Cisco 3600 series.
12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T and implemented on the Cisco IAD2420 series.

Examples

The following example configures a voice port with immediate-start signaling enabled:

```
Router# voice-port 1/17
Router (config-voiceport)# signal did immediate-start
```

signal keepalive

To configure the keepalive signaling packet interval for Cisco trunks and FRF.11 trunks, use the **signal keepalive** command in voice-class configuration mode. To reset to the default, use the **no** form of this command.

signal keepalive {*seconds* | **disabled**}
no signal keepalive {*seconds* | **disabled**}

Syntax Description

seconds	Keepalive signaling packet interval, in seconds. Range is from 1 to 65535. Default is 5 seconds.
disabled	Specifies that no keepalive signals are sent.

Command Default

seconds : 5 seconds

Command Modes

Voice-class configuration (config-voice-class)

Command History

Release	Modification
12.0(3)XG	This command was introduced on the Cisco MC3810.
12.0(4)T	This command was integrated into Cisco IOS Release 12.0(4)T.
12.1(3)T	This command was implemented on the Cisco 2600 series and Cisco 3600 series.
12.3(7)T	The **disabled** keyword was added.

Usage Guidelines

Before configuring the keepalive signaling interval, you must use the **voice class permanent** command in global configuration mode to create a voice class for the Cisco trunk or FRF.11 trunk. The voice class must then be assigned to a dial peer using the **voice-class permanent** (dial-peer) command.

To avoid sending keepalive signals to a multicasting network with no specified destination, we recommend that you use the **disabled**keyword when configuring this command for use in networks that use connection trunk connections and multicasting.

Examples

The following example shows the keepalive signaling interval set to 3 seconds for voice class 10:

```
voice class permanent 10
 signal keepalive 3
 exit
dial-peer voice 100 vofr
 voice-class permanent 10
```

Related Commands

Command	Description
dial-peer voice	Enters dial-peer configuration mode and specifies a dial-peer type.
signal pattern	Configures the ABCD bit pattern for Cisco trunks and FRF.11 trunks.

Command	Description
signal timing idle suppress-voice	Configures the signal timing parameter for the idle state of a call.
signal timing oos	Configures the signal timing parameter for the OOS state of a call.
voice-class permanent	Creates a voice class for a Cisco trunk or FRF.11 trunk.
voice class permanent	Assigns a previously-configured voice class for a Cisco trunk or FRF.11 trunk to a dial peer.

signal pattern

To define the ABCD bit patterns that identify the idle and out-of-service (OOS) states for Cisco trunks and FRF.11 trunks, use the **signal pattern** command in voice-class configuration mode. To remove the patterns from the voice class, use the **no** form of this command.

signal pattern {**idle receive** | **idle transmit** | **oos receive** | **oos transmit**} *bit-pattern*
no signal pattern {**idle receive** | **idle transmit** | **oos receive** | **oos transmit**} *bit-pattern*

Syntax Description

idle receive	Signaling pattern for identifying an idle message from the network. Also defines the idle signaling pattern to be sent to the PBX if the network trunk is out of service and the **signal sequence oos idle-only** or **signal sequence oos both** command is configured.
idle transmit	Signaling pattern for identifying an idle message from the PBX.
oos receive	OOS signaling pattern to be sent to the PBX if the network trunk is out of service and the **signal sequence oos oos-only** or **signal sequence oos both** command is configured.
oos transmit	Signaling pattern for identifying an OOS message from the PBX.
bit -pattern	ABCD bit pattern. Range is from 0000 to 1111.

Command Default

idle receive	Near-end E&M: 0000 (for T1) or 0001 (for E1) Near-end FXO loop start: 0101 Near-end FXO ground start: 1111 Near-end FXS: 0101 Near-end MELCAS: 1101
idle transmit	Near-end E&M: 0000 Near-end FXO: 0101 Near-end FXS loop start: 0101 Near-end FXS ground start: 1111 Near-end MELCAS: 1101
oos receive	Near-end E&M: 1111 Near-end FXO loop start: 1111 Near-end FXO ground start: 0000 Near-end FXS loop start: 1111 Near-end FXS ground start: 0101 Near-end MELCAS: 1111
oos transmit	No default signaling pattern is defined.

Command Modes

Voice-class configuration (config-voice-class)

Command History

Release	Modification
12.0(3)XG	This command was introduced on the Cisco MC3810.
12.0(4)T	This command was integrated into Cisco IOS Release 12.0(4)T.
12.0(7)XK	Default signaling patterns were defined.
12.1(2)T	This command was integrated into Cisco IOS Release 12.1(2)T.
12.1(3)T	This command was implemented on the Cisco 2600 series and Cisco 3600 series.

Usage Guidelines

Before configuring the signaling pattern, you must use the **voice-class permanent** command in global configuration mode to create a voice class for the Cisco trunk or FRF.11 trunk. After you define the voice class, you assign it to a dial peer.

Idle Patterns

An idle state is generated if the router detects an idle signaling pattern coming from either direction. If an idle pattern is configured for only one direction (transmit or receive), an idle state can be detected only in the configured direction. Therefore, you should normally enter both the **idle receive** and the **idle transmit** keywords.

To suppress voice packets whenever the transmit or receive trunk is in the idle state, use the **idle receive** and **idle transmit** keywords in conjunction with the **signal timing idle suppress-voice** command.

OOS Patterns

An OOS state is generated differently in each direction under the following conditions:

- If the router detects an **oos transmit** signaling pattern sent from the PBX, the router transmits the **oos transmit** signaling pattern to the network.
- If the **signal timing oos timeout** timer expires and the router receives no signaling packets from the network (network is OOS), the router sends an **oos receive** signaling pattern to the PBX. (The **oos receive** pattern is not matched against the signaling packets received from the network; the receive packets indicate an OOS condition directly by setting the AIS alarm indication bit in the packet.)

To suppress voice packets whenever the transmit or receive trunk is in the OOS state, use the **oos receive** and **oos transmit**keywords in conjunction with the **signal timing oos suppress-voice** command.

To suppress voice and signaling packets whenever the transmit or receive trunk is in the OOS state, use the **oos receive** and **oos transmit** keywords in conjunction with the **signal timing oos suppress-all** command.

PBX Busyout

To "busy out" a PBX if the network connection fails, set the **oos receive** pattern to match the seized state (busy), and set the **signal timing oos** timeout value. When the timeout value expires and no signaling packets are received, the router sends the **oos receive** pattern to the PBX.

Use the busy seized pattern only if the PBX does not have a specified pattern for indicating an OOS state. If the PBX has a specific OOS pattern, use that pattern instead.

Examples

The following example, beginning in global configuration mode, configures the signaling bit pattern for the idle receive and transmit states:

```
voice class permanent 10
 signal keepalive 3
 signal pattern idle receive 0101
 signal pattern idle transmit 0101
 exit
dial-peer voice 100 vofr
 voice-class permanent 10
```

The following example, beginning in global configuration mode, configures the signaling bit pattern for the out-of-service receive and transmit states:

```
voice class permanent 10
 signal keepalive 3
 signal pattern oos receive 0001
```

```
 signal pattern oos transmit 0001
 exit
dial-peer voice 100 vofr
 voice-class permanent 10
```

The following example restores default signaling bit patterns for the receive and transmit idle states:

```
voice class permanent 10
 signal keepalive 3
 signal timing idle suppress-voice
 no signal pattern idle receive
 no signal pattern idle transmit
 exit
dial-peer voice 100 vofr
 voice-class permanent 10
```

The following example configures nondefault signaling bit patterns for the receive and transmit out-of-service states:

```
voice class permanent 10
 signal keepalive 3
 signal pattern oos receive 0001
 signal pattern oos transmit 0001
 exit
dial-peer voice 100 vofr
 voice-class permanent 10
```

Related Commands

Command	Description
dial-peer voice	Enters dial-peer configuration mode and specifies a dial-peer type.
signal timing idle suppress-voice	Specifies the length of time before voice traffic is stopped after a trunk goes into the idle state.
signal timing oos	Configures the signal timing parameter for the OOS call state.
signal timing oos standby	Specifies that a secondary port return to its initial standby state after the trunk has been OOS for a specified time.
signal timing oos suppress-all	Stops sending voice and signaling packets to the network if a transmit OOS signaling pattern id detected from the PBX for a specified time.
signal timing oos suppress-voice	Stops sending voice packets to the network if a transmit OOS signaling pattern is detected from the PBX for a specified time.
signal timing oos timeout	Changes the delay time between the loss of signaling packets from the network and the start time for the OOS state.
voice-class permanent	Creates a voice class for a Cisco trunk or FRF.11 trunk.
voice class permanent	Assigns a previously-configured voice class for a Cisco trunk or FRF.11 trunk to a dial peer.

signal sequence oos

To specify which signaling pattern is sent to the PBX when the far-end keepalive message is lost or an alarm indication signal (AIS) is received from the far end, use the **signal sequence oos** command in voice-class configuration mode. To reset to the default, use the **no** form of this command.

signal sequence oos {**no-action** | **idle-only** | **oos-only** | **both**}
no signal sequence oos

Syntax Description

no -action	No signaling pattern is sent.
idle -only	Only the idle signaling pattern is sent.
oos -only	Only the out-of-service (OOS) signaling pattern is sent.
both	Both idle and OOS signaling patterns are sent. This is the default value.

Command Default

Both idle and OOS signaling patterns are sent.

Command Modes

Voice-class configuration

Command History

Release	Modification
12.0(7)XK	This command was introduced on the Cisco MC3810.
12.1(2)T	This command was integrated into Cisco IOS Release 12.1(2)T.
12.1(3)T	This command was implemented on the Cisco 2600 series and Cisco 3600 series.

Usage Guidelines

Before configuring the idle or OOS signaling patterns to be sent, you must use the **voice class permanent** command in global configuration mode to create a voice class for the Cisco trunk or FRF.11 trunk. After you finish defining the voice class, you assign it to a dial peer.

Use the **signal sequence oos** command to specify which signaling pattern) to send. Use the **signal pattern idle receive** or the **signal pattern oos receive** command to define the bit patterns of the signaling patterns if other than the defaults.

Examples

The following example, beginning in global configuration mode, defines voice class 10, sets the **signal sequence oos**command to send only the idle signal pattern to the PBX, and applies the voice class configuration to VoFR dial peer 100.

```
voice-class permanent 10
 signal-keepalive 3
 signal sequence oos idle-only
 signal timing idle suppress-voice
 exit
dial-peer voice 100 vofr
 voice-class permanent 10
 signal-type transparent
```

Related Commands

Command	Description
dial-peer voice	Enters dial-peer configuration mode and specifies a dial-peer type.
signal pattern	Configures the ABCD bit pattern for Cisco trunks and FRF.11 trunks.
signal timing idle suppress-voice	Specifies the length of time before the router stops sending voice packets after a trunk goes into the idle state.
signal timing oos	Specifies that a permanent voice connection be torn down and restarted after the trunk has been OOS for a specified time.
signal timing oos standby	Specifies that a port return to its initial standby state after the trunk has been OOS for a specified time.
signal timing oos suppress-all	Configures the router or concentrator to stop sending voice and signaling packets to the network if it detects an OOS signaling pattern from the PBX for a specified time.
signal timing oos suppress-voice	Configures the router or concentrator to stop sending voice packets to the network if it detects a transmit OOS signaling pattern from the PBX for a specified time.
signal timing oos timeout	Changes the delay time between the loss of signaling packets from the network and the start time for the OOS state.
voice-class permanent	Creates a voice class for a Cisco trunk or FRF.11 trunk.
voice class permanent	Assigns a previously-configured voice class for a Cisco trunk or FRF.11 trunk to a dial peer.

signal timing idle suppress-voice

To configure the signal timing parameter for the idle state of a call, use the s**ignal timing idle suppress-voice** command in voice-class configuration mode. To reset to the default, use the **no** form of this command.

signal timing idle suppress-voice *seconds* [**resume-voice** [*milliseconds*]]
no signal timing idle suppress-voice *seconds* [**resume-voice** [*milliseconds*]]

Syntax Description

seconds	Duration of the idle state, in seconds, before the voice traffic is stopped. Range is from 0 to 65535.
resume-voice	(Optional) Sets a timer that controls the delay between when trunk activity is detected and when active packetization of voice resumes.
milliseconds	(Optional) Duration of the delay, in milliseconds (ms), for the resume-voice timer. Range is from 40 to 5000. Default is 500 ms.

Command Default

No signal timing idle suppress-voice timer is configured.

Command Modes

Voice-class configuration (config-voice-class)

Command History

Release	Modification
12.0(3)XG	This command was introduced on the Cisco MC3810 platform.
12.0(4)T	This command was integrated into Cisco IOS Release 12.0(4)T.
12.0(7)XK	This command was modified to simplify the configuration process.
12.1(2)T	This command was integrated into Cisco IOS Release 12.1(2)T.
12.1(3)T	This command was implemented on the Cisco 2600 series and Cisco 3600 series.
12.4(15)T10	This command was modified to add the **resume-voice** *milliseconds* option.

Usage Guidelines

Before configuring the signal timing idle suppress-voice timer, you must use the **voice class permanent** command in global configuration mode to create a voice class for the Cisco trunk or FRF.11 trunk. The voice class must then be assigned to a dial peer.

The **signal timing idle suppress-voice**command is used when the **signal-type** command is set to **transparent** in the dial peer for the Cisco trunk or FRF.11 trunk connection. The router stops sending voice packets when the timer expires. Signaling packets are still sent.

To detect an idle trunk state, the router or concentrator monitors both transmit and receive signaling for the idle transmit and idle receive signaling patterns. These can be configured by the **signal pattern idle transmit** or **signal pattern idle receive** command, or they can be the defaults. The default idle receive pattern is the idle pattern of the local voice port. The default idle transmit pattern is the idle pattern of the far-end voice port.

In some circumstances, the default delay of 500 ms between the detection of incoming seizure and the opening of the audio path may cause a timing issue.

If, during this delay of 500 ms, the near-end originating PBX has already received the acknowledgement from the far-end PBX to begin playing out digits and the audio path is not yet open, the first Dual Tone Multi-Frequency (DTMF) digit might be lost over the permanent trunk.

This loss of the first DTMF digit can occur if a Cisco voice gateway has the following trunk conditioning setting:

```
!
voice class permanent 1
signal pattern idle transmit 0000
signal pattern idle receive 0000
signal pattern oos transmit 1111
signal pattern oos receive 1111
signal timing idle suppress-voice 10
!
```

The **resume-voice** *milliseconds* option has been added in Release 12.4(15)T10 to modify the delay timer and reduce the wait time. We recommend that you specify a delay of less than 500 ms to avoid the loss of any digits due to the possible discrepancy between the detection of incoming seizure and the opening of the audio path.

The output of the **show voice trunk-conditioning supervisory** command has been modified in Release 12.4(15)T10 to report values for the **suppress-voice** and **resume-voice** keywords (of the **signal timing idle suppress-voice** command) as the "idle = *seconds* " and "idle_off = *milliseconds* " fields, respectively.

Examples

The following example, beginning in global configuration mode, sets the signal timing idle suppress-voice timer to 5 seconds for the idle state on voice class 10:

```
voice class permanent 10
 signal keepalive 3
 signal pattern idle receive 0101
 signal pattern idle transmit 0101
 signal timing idle suppress-voice 5
 exit
 dial-peer voice 100 vofr
 voice-class permanent 10
 signal-type transparent
```

The following example defines voice class 10, sets the idle detection time to 5 seconds, configures the trunk to use the default transmit and receive idle signal patterns, and applies the voice class configuration to VoFR dial peer 100:

```
voice class permanent 10
 signal keepalive 3
 signal timing idle suppress-voice 5
 exit
dial-peer voice 100 vofr
 voice-class permanent 10
 signal-type transparent
```

Related Commands

Command	Description
dial-peer voice	Enters dial-peer configuration mode and specifies the method of voice encapsulation.
show voice trunk-conditioning supervisory	Displays the status of trunk supervision and configuration parameters for a voice port.
signal keepalive	Configures the keepalive signaling packet interval for Cisco trunks and FRF.11 trunks.
signal pattern	Defines the ABCD bit patterns that identify the idle and OOS states for Cisco trunks and FRF.11 trunks.
signal timing oos	Configures the signal timing parameter for the OOS state of a call.
signal-type	Sets the signaling type to be used when connecting to a dial peer.
voice-class permanent	Creates a voice class for a Cisco trunk or FRF.11 trunk.
voice class permanent (dial peer)	Assigns a previously configured voice class for a Cisco trunk or FRF.11 trunk to a dial peer.

signal timing oos

To configure the signal timing parameter for the out-of-service (OOS) state of the call, use the **signal timing oos**command in voice-class configuration mode. To reset to the default, use the **no** form of this command.

signal timing oos { **restart** | **standby** | **suppress-all** | **suppress-voice** | **timeout** } *seconds*
no signal timing oos { **restart** | **standby** | **suppress-all** | **suppress-voice** | **timeout** } *seconds*

Syntax Description

restart	If no signaling packets are received for this period, the permanent voice connection is torn down and an attempt to achieve reconnection is made.
standby	If no signaling packets are received for this period, a secondary port returns to its initial standby state. This option applies only to secondary ports (ports configured using the **connection trunk** *number* **answer-mode** command).
suppress -all	If the transmit OOS pattern (from the PBX to the network) matches for this period of time, the router stops sending all packets to the network.
suppress -voice	If the transmit OOS pattern (from the PBX to the network) matches for this period of time, the router stops sending voice packets to the network. signaling packets continue to be sent with the alarm indication set (AIS).
timeout	If no signaling packets are received for this period of time, the router sends the configured receive OOS pattern to the PBX. Also, the router stops sending voice packets to the network. Use this option to perform busyout to the PBX.
seconds	Duration, in seconds, for the above settings. Range is from 0 to 65535.

Command Default

No signal timing OOS pattern parameters are configured.

Command Modes

Voice-class configuration (config-voice-class)

Command History

Release	Modification
12.0(4)T	This command was introduced.

Usage Guidelines

Before configuring signal timing OOS parameters, you must use the **voice class permanent** command in global configuration mode to create a voice class for the Cisco trunk or FRF.11 trunk. The voice class must then be assigned to a dial peer.

You can enter several values for this command. However, the **suppress-all** and **suppress-voice** options are mutually exclusive.

Examples

The following example, beginning in global configuration mode, configures the signal timeout parameter for the OOS state on voice class 10. The **signal timing oos timeout**command is set to 60 seconds.

```
voice-class permanent 10
```

```
 signal-keepalive 3
 signal pattern oos receive 0001
 signal pattern oos transmit 0001
 signal timing oos timeout 60
 exit
dial-peer voice 100 vofr
 voice-class permanent 10
```

Related Commands

Command	Description
connection	Specifies a connection mode for a voice port.
dial-peer voice	Enters dial-peer configuration mode and specifies the method of voice encapsulation.
signal keepalive	Configures the keepalive signaling packet interval for Cisco trunks and FRF.11 trunks.
signal pattern	Defines the ABCD bit patterns that identify the idle and oos states for Cisco trunks and FRF.11 trunks.
signal timing idle suppress-voice	Configures the signal timing parameter for the idle state of the call.
signal-type	Sets the signaling type to be used when connecting to a dial peer.
voice class permanent	Creates a voice class for a Cisco trunk or FRF.11 trunk.
voice-class permanent (dial-peer)	Assigns a previously configured voice class for a Cisco trunk or FRF.11 trunk to a dial peer.

signal timing oos restart

To specify that a permanent voice connection be torn down and restarted after the trunk has been out-of-service (OOS) for a specified time, use the **signal timing oos restart** command in voice-class configuration mode. To reset to the default, use the **no** form of this command.

signal timing oos restart *seconds*
no signal timing oos restart

Syntax Description

seconds	Delay duration, in seconds, for the restart attempt. Range is from 0 to 65535. There is no default.

Command Default

No restart attempt is made if the trunk becomes OOS.

Command Modes

Voice-class configuration (config-voice-class)

Command History

Release	Modification
12.0(3)XG	This command was introduced on the Cisco MC3810.
12.0(4)T	This command was integrated into Cisco IOS Release 12.0(4)T.
12.1(3)T	This command was implemented on the Cisco 2600 series and Cisco 3600 series.

Usage Guidelines

Before configuring signal timing OOS parameters, you must use the **voice class permanent** command in global configuration mode to create a voice class for the Cisco trunk or FRF.11 trunk. You then assign the voice class to a dial peer.

The **signal timing oos restart** command is valid only if the **signal timing oos timeout** command is enabled, which controls the start time for the OOS state. The timer for the **signal timing oos restart** command does not start until the trunk is OOS.

Examples

The following example, beginning in global configuration mode, creates voice class 10, sets the OOS **timeout** time to 60 seconds and sets the **restart** time to 30 seconds:

```
voice-class permanent 10
 signal-keepalive 3
 signal pattern oos receive 0001
 signal pattern oos transmit 0001
 signal timing oos timeout 60
 signal timing oos restart 30
 exit
dial-peer voice 100 vofr
 voice-class permanent 10
```

Related Commands

Command	Description
connection	Specifies a connection mode for a voice port.

Command	Description
dial-peer voice	Enters dial-peer configuration mode and specifies the method of voice encapsulation.
signal keepalive	Configures the keepalive signaling packet interval for Cisco trunks and FRF.11 trunks.
signal pattern	Defines the ABCD bit patterns that identify the idle and oos states for Cisco trunks and FRF.11 trunks.
signal timing idle suppress-voice	Configures the signal timing parameter for the idle state of a call.
signal-type	Sets the signaling type to be used when connecting to a dial peer.
voice class permanent	Creates a voice class for a Cisco trunk or FRF.11 trunk.
voice-class permanent (dial-peer)	Assigns a previously-configured voice class for a Cisco trunk or FRF.11 trunk to a dial peer.

signal timing oos standby

To configure a secondary port to return to its initial standby state after the trunk has been out-of-service (OOS) for a specified time, use the **signal timing oos standby** command in voice-class configuration mode. To reset to the default, use the **no** form of this command.

signal timing oos standby *seconds*
no signal timing oos standby

Syntax Description

seconds	Delay duration, in seconds. If no signaling packets are received for this period, the secondary port returns to its initial standby state. Range is from 0 to 65535. There is no default.

Command Default

The secondary port does not return to its standby state if the trunk becomes OOS.

Command Modes

Voice-class configuration (config-voice-class)

Command History

Release	Modification
12.0(3)XG	This command was introduced on the Cisco MC3810.
12.0(4)T	This command was integrated into Cisco IOS Release 12.0(4)T.
12.1(3)T	This command was implemented on the Cisco 2600 series and Cisco 3600 series.

Usage Guidelines

Before configuring signal timing OOS parameters, you must use the **voice class permanent**command in global configuration mode to create a voice class for the Cisco trunk or FRF.11 trunk. After you finish defining the voice class, you assign it to a dial peer.

If no signaling packets are received for the specified delay period, the secondary port returns to its initial standby state. The **signal timing oos standby** command is valid only if both of the following conditions are true:

- The **signal timing oos timeout** command is enabled, which controls the start time for the OOS state. The timer for the **signal timing oos standby** command does not start until the trunk is OOS.
- The voice port is configured as a secondary port with the **connection trunk** *digits* **answer-mode** command.

Examples

The following example, beginning in global configuration mode, creates a voice port as a secondary voice port, creates voice class 10, sets the OOS **timeout** time to 60 seconds, and sets the return-to-**standby** time to 120 seconds:

```
4351-Router #signal timing oos standby ?
  <0-65535>  Time in seconds
4351-Router #signal timing oos standby
```

Related Commands

Command	Description
connection	Specifies a connection mode for a voice port.

Command	Description
dial-peer voice	Enters dial-peer configuration mode and specifies the method of voice encapsulation.
signal keepalive	Configures the keepalive signaling packet interval for Cisco trunks and FRF.11 trunks.
signal pattern	Defines the ABCD bit patterns that identify the idle and oos states for Cisco trunks and FRF.11 trunks.
signal timing idle suppress-voice	Configures the signal timing parameter for the idle state of a call.
signal-type	Sets the signaling type to be used when connecting to a dial peer.
voice class permanent	Creates a voice class for a Cisco trunk or FRF.11 trunk.
voice-class permanent (dial-peer)	Assigns a previously configured voice class for a Cisco trunk or FRF.11 trunk to a dial peer.

signal timing oos suppress-all

To configure the router or concentrator to stop sending voice and signaling packets to the network if it detects a transmit out-of-service (OOS) signaling pattern from the PBX for a specified time, use the **signal timing oos suppress-all** command in voice-class configuration mode. To reset to the default, use the **no** form of this command.

signal timing oos suppress-all *seconds*
no signal timing oos suppress-all

Syntax Description

seconds	Delay duration, in seconds, before packet transmission is stopped. Range is from 0 to 65535. There is no default.

Command Default

The router or concentrator does not stop sending packets to the network if it detects a transmit OOS signaling pattern from the PBX.

Command Modes

Voice-class configuration (config-voice-class)

Command History

Release	Modification
12.0(3)XG	This command was introduced on the Cisco MC3810.
12.0(4)T	This command was integrated into Cisco IOS Release 12.0(4)T.
12.1(3)T	This command was implemented on the Cisco 2600 series and Cisco 3600 series.

Usage Guidelines

Before configuring signal timing OOS parameters, you must use the **voice class permanent** command in global configuration mode to create a voice class for the Cisco trunk or FRF.11 trunk. After you finish defining the voice class, you assign it to a dial peer.

The **signal timing oos suppress-all** command is valid only if you configure an OOS transmit signaling pattern with the **signal pattern oos transmit** command. (There is no default **oos transmit** signaling pattern.)

The **signal timing oos suppress-all** command is valid whether or not the **signal timing oos timeout** command is enabled, which controls the start time for the OOS state. The timer for the **signal timing oos suppress-all** command starts immediately when the OOS transmit signaling pattern is matched.

Examples

The following example, beginning in global configuration mode, creates voice class 10, sets the OOS **timeout** time to 60 seconds, and sets the packet suppression time to 60 seconds:

```
voice-class permanent 10
 signal-keepalive 3
 signal pattern oos receive 0001
 signal pattern oos transmit 0001
 signal timing oos timeout 60
 signal timing oos suppress-all 60
 exit
dial-peer voice 100 vofr
 voice-class permanent 10
```

Related Commands

Command	Description
connection	Specifies a connection mode for a voice port.
dial-peer voice	Enters dial-peer configuration mode and specifies the method of voice encapsulation.
signal keepalive	Configures the keepalive signaling packet interval for Cisco trunks and FRF.11 trunks.
signal pattern	Defines the ABCD bit patterns that identify the idle and oos states for Cisco trunks and FRF.11 trunks.
signal timing idle suppress-voice	Configures the signal timing parameter for the idle state of a call.
signal-type	Sets the signaling type to be used when connecting to a dial peer.
voice class permanent	Creates a voice class for a Cisco trunk or FRF.11 trunk.
voice-class permanent (dial-peer)	Assigns a previously configured voice class for a Cisco trunk or FRF.11 trunk to a dial peer.

signal timing oos suppress-voice

To configure the router or concentrator to stop sending voice packets to the network if it detects a transmit out-of-service (OOS) signaling pattern from the PBX for a specified time, use the **signal timing oos suppress-voice** command in voice-class configuration mode. To reset to the default, use the **no** form of this command.

signal timing oos suppress-voice *seconds*
no signal timing oos suppress-voice

Syntax Description

seconds	Delay duration, in seconds, before voice-packet transmission is stopped. Range is from 0 to 65535. There is no default.

Command Default

The router or concentrator does not stop sending voice packets to the network if it detects a transmit OOS signaling pattern from the PBX.

Command Modes

Voice-class configuration (config-voice-class)

Command History

Release	Modification
12.0(3)XG	This command was introduced on the Cisco MC3810.
12.0(4)T	This command was integrated into Cisco IOS Release 12.0(4)T.
12.1(3)T	This command was implemented on the Cisco 2600 series and Cisco 3600 series.

Usage Guidelines

Before configuring signal timing OOS parameters, you must use the **voice class permanent** command in global configuration mode to create a voice class for the Cisco trunk or FRF.11 trunk. After you finish defining the voice class, you assign it to a dial peer.

The **signal timing oos suppress-voice** command is valid only if you configure an OOS transmit signaling pattern with the **signal pattern oos transmit** command. (There is no default **oos transmit** signaling pattern.)

The **signal timing oos suppress-voice** s command is valid whether or not the **signal timing oos timeout**command is enabled, which controls the start time for the OOS state. The timer for the **signal timing oos suppress-voice** command starts immediately when the OOS transmit signaling pattern is matched.

Examples

The following example, beginning in global configuration mode, creates voice class 10, sets the OOS **timeout** time to 60 seconds, and sets the packet suppression time to 60 seconds:

```
voice-class permanent 10
 signal-keepalive 3
 signal pattern oos receive 0001
 signal pattern oos transmit 0001
 signal timing oos timeout 60
 signal timing oos suppress-voice 60
 exit
dial-peer voice 100 vofr
 voice-class permanent 10
```

Related Commands

Command	Description
connection	Specifies a connection mode for a voice port.
dial-peer voice	Enters dial-peer configuration mode and specifies the method of voice encapsulation.
signal keepalive	Configures the keepalive signaling packet interval for Cisco trunks and FRF.11 trunks.
signal pattern	Defines the ABCD bit patterns that identify the idle and oos states for Cisco trunks and FRF.11 trunks.
signal timing idle suppress-voice	Configures the signal timing parameter for the idle state of a call.
signal-type	Sets the signaling type to be used when connecting to a dial peer.
voice class permanent	Creates a voice class for a Cisco trunk or FRF.11 trunk.
voice-class permanent (dial-peer)	Assigns a previously configured voice class for a Cisco trunk or FRF.11 trunk to a dial peer.

signal timing oos timeout

To change the delay time between the loss of signaling packets from the network and the start time for the out-of-service (OOS) state, use the **signal timing oos timeout** command in voice-class configuration mode. To reset to the default, use the **no** form of this command.

signal timing oos timeout [*seconds* | **disabled**]
no signal timing oos timeout

Syntax Description

seconds	(Optional) Delay duration, in seconds, between the loss of signaling packets and the beginning of the OOS state. Range is from 1 to 65535. Default is 30.
disabled	(Optional) Deactivates the detection of packet loss. If no signaling packets are received from the network, the router does not sent an OOS pattern to the PBX and it continues sending voice packets to the network. Use this option to disable busyout to the PBX.

Command Default

No signal timing OOS pattern parameters are configured.

Command Modes

Voice-class configuration

Command History

Release	Modification
12.0(3)XG	This command was introduced on the Cisco MC3810.
12.0(4)T	This command was integrated into Cisco IOS Release 12.0(4)T.
12.1(3)T	This command was implemented on the Cisco 2600 series and Cisco 3600 series.

Usage Guidelines

Before configuring signal timing OOS parameters, you must use the **voice class permanent** command in global configuration mode to create a voice class for the Cisco trunk or FRF.11 trunk. After you finish defining the voice class, you assign it to a dial peer.

You can use the **signal timing oos timeout**command to enable busyout to the PBX.

The **signal timing oos timeout**command controls the starting time for the **signal timing oos restart** and **signal timing oos -standby** commands. If this command is entered with the **disabled** keyword, the **signal timing oos restart** and **signal timing oos standby** commands are ineffective.

Examples

The following example, beginning in global configuration mode, creates voice class 10 and sets the OOS **timeout** time to 60 seconds:

```
voice-class permanent 10
 signal-keepalive 3
 signal pattern oos receive 0001
 signal pattern oos transmit 0001
 signal timing oos timeout 60
 exit
dial-peer voice 100 vofr
 voice-class permanent 10
```

Related Commands

Command	Description
connection	Specifies a connection mode for a voice port.
dial-peer voice	Enters dial-peer configuration mode and specifies the method of voice encapsulation.
signal keepalive	Configures the keepalive signaling packet interval for Cisco trunks and FRF.11 trunks.
signal pattern	Defines the ABCD bit patterns that identify the idle and oos states for Cisco trunks and FRF.11 trunks.
signal timing idle suppress-voice	Configures the signal timing parameter for the idle state of a call.
signal-type	Sets the signaling type to be used when connecting to a dial peer.
voice class permanent	Creates a voice class for a Cisco trunk or FRF.11 trunk.
voice-class permanent (dial-peer)	Assigns a previously configured voice class for a Cisco trunk or FRF.11 trunk to a dial peer.

signaling forward

To configure global settings for transparent tunneling of Q-signaling (QSIG), Q.931, H.225, and ISDN User Part (ISUP) messages on a Cisco IOS voice gateway, use the **signaling forward** command in voice service VoIP configuration mode. To return to the default tunneling configuration for a gateway, use the **no** form of this command.

Cisco IOS H.323 Gateways
signaling forward {**conditional** | **none** | **rawmsg** | **unconditional**}
no signaling forward

Cisco IOS SIP Gateways
signaling forward {**none** | **rawmsg** | **unconditional**}
no signaling forward

Syntax Description

conditional	Specifies that tunneling on an H.323 gateway is determined by the target, which is defined using the **session target** command. This is the default setting for H.323 gateways. **Note** The **conditional** keyword is not supported on Session Initiation Protocol (SIP) gateways. Instead, the default setting for SIP gateways is that no tunneling is configured (**none**).
none	Specifies that H.323 and SIP gateways do not forward Generic Transparency Descriptor (GTD), QSIG, or Q.931 payloads to any endpoint in the network. This is the default setting for SIP gateways.
rawmsg	Specifies that H.323 and SIP gateways tunnel H.225, QSIG (application-qsig), or Q.931 raw messages (application-Xq931) only, without GTD.
unconditional	Specifies unconditional tunneling and forwards GTD payload along with the QSIG or Q.931 message body even if the attached external route server has modified it. (The gatekeeper sends its own GTD back to itself.)

Command Default

- **conditional** --messages are forwarded according to the target:
  - Non-Registration, Admission, and Status (RAS) targets--only the original payload (without GTD) is forwarded to the H.323 endpoint.
  - All other targets--GTD payload is forwarded along with the message body.

No transparent tunneling of QSIG or Q.931 messages is configured.

Command Modes

Voice service VoIP configuration (conf-voi-serv)

SIP UA configuration (config-sip-ua)

Command History

Release	Modification
12.2(11)T	This command was introduced.

Release	Modification
12.3(1)	Support was added for SIP Public Switched Telephone Network (PSTN) transport using Cisco GTD.
12.4(15)XY	Support was added for passing RELEASE and RELEASE COMPLETE messages end to end over SIP using QSIG tunneling on Cisco IOS voice gateways.
12.4(15)XZ	Support was added for Q.931 tunneling over SIP on Cisco IOS voice gateways and tunneling of both QSIG and Q.931 over SIP was extended to the Cisco Unified Border Element (CUBE). **Note** The CUBE is formerly known as the Cisco IOS Session Border Controller (SBC) or the Cisco Multiservice IP-to-IP Gateway.
12.4(20)T	Support was added for QSIG and Q.931 tunneling over SIP on Cisco IOS voice gateways and the CUBE.
Cisco IOS XE Cupertino 17.7.1a	Introduced support for YANG models.

Usage Guidelines

This command is used on H.323 and SIP voice gateways to configure tunneling behavior. Depending on your specific Cisco router, platform, and network, you can use this command to configure tunneling behavior for various messages, such as QSIG, Q.931, H.225, and ISUP messages. To override the global setting for a gateway or to configure tunneling settings on a dial peer, use the **signaling forward** command in dial peer voice configuration mode.

For more specific information about controlling tunneling behavior using the **signaling forward** command, see the information included in the following sections:

QSIG and Q.931 Tunneling

Tunneling of QSIG and Q.931 on H.323 gateways is enabled by default for Cisco IOS gateway platforms supporting the **signaling forward** command. For QSIG and Q.931 tunneling on SIP gateways, however, you must configure at least one interface on both an ingress, or originating gateway (OGW), and an egress, or terminating gateway (TGW).

In addition to signaling forward settings, you must specify QSIG or Q.931 as the central office switch type on the ISDN interface for both the OGW and TGW on a SIP or H.323 network. Use the **isdn switch-type** command to enable and specify the switch type:

- For tunneling QSIG messages, specify the **primary-qsig** switch type.
- For tunneling Q.931 messages, specify any ISDN switch type except **primary-qsig** and **primary-dpness**.



Note Cisco IOS SIP gateways do not support the **primary-dpness** switch type for tunneling of Q.931.

The table below displays QSIG and Q.931 tunneling behavior as determined by gateway voice class and configuration settings.

Table 223: QSIG Tunneling Behavior by Voice Class and Signaling Forward Setting

Signaling Forward Configuration	H.323 Gateway	SIP Gateway
conditional or no specified setting:	Default.	Not supported.
session target *non-ras*	Tunnels GTD payload with QSIG or Q.931 message bodies.	No tunneling.
session target ras	Tunnels only QSIG or Q.931 message bodies.	No tunneling.
none	No tunneling.	No tunneling.
rawmsg	Tunnels QSIG or Q.931 message bodies only.	Tunnels QSIG or Q.931 message bodies only.
unconditional	Tunnels GTD payload along with QSIG or Q.931 message bodies.	Tunnels GTD payload along with QSIG or Q.931 message bodies.

SS7 ISUP and H.225 Tunneling over H.323

ISUP defines the protocol and procedures used to configure, manage, and release trunk circuits that carry voice and data calls over the PSTN. ISUP is used for both ISDN and non-ISDN calls and is reconstructed on the basis of the protocol at the egress side of the network, without any concern for the ISDN or ISUP variant on the ingress side of the network.

When you specify that the ISDN (H.225) or ISUP information be provided in text format, the information can also be used by applications inside the core H.323 network such as, in a route server, which can use certain ISDN and ISUP information for routing decisions. Additionally, transporting ISUP encapsulated in GTD maintains compatibility with the H.323 protocol.

If the target is a RAS target, for a non-GTD signaling payload, the original payload is forwarded. For a GTD signaling payload, the payload is encapsulated in an admission request (ARQ)/disengage request (DRQ) message and sent to the originating gatekeeper. The gatekeeper conveys the payload to the Gatekeeper Transaction Message Protocol (GKTMP) and external route server for a flexible route decision based upon the ISUP GTD parameters. The gateway then conditionally forwards the GTD payload on the basis of the instruction from the route server.

To tunnel the ISUP GTD, you must configure the OGW and TGW to encapsulate SS7 ISUP messages in GTD format.

Note If you specify **primary-qsig** as the **isdn switch-type** setting, you must assign network-side functionality (either at the global or dial-peer level) using the **isdn protocol-emulate** command.

Examples

The following example shows unconditional signal forwarding being set on a global basis, where the GTD payload is tunneled to endpoints over either H.323 or SIP:

```
Router> enable
```

```
Router# configure
 terminal
Router(config)# voice service voip
Router(conf-voi-serv)# signaling forward unconditional
```

The following example is sample output from the **show running-config** command when a router is globally configured with unconditional signal forwarding over SIP:

```
Router# show running-config
Building configuration...
Building configuration...
Current configuration : 2357 bytes
!
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
!
!
.
.
!
voice service voip
 signaling forward unconditional
 sip
!
.
.
```

The following example is sample output from the **show running-config** command when a router is globally configured with unconditional signal forwarding over H.323:

```
Router# show running-config
Building configuration...
Current configuration : 4201 bytes
!
version 12.2
service config
no service single-slot-reload-enable
no service pad
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
service internal
service udp-small-servers
!
hostname as5300-2
!
no logging buffered
logging rate-limit console 10 except errors
aaa new-model
!
.
.
.
!
voice service voip
 signaling forward unconditional
 h323
!
.
```

.
.

Related Commands

clid network-number	Configures a network number in the router for CLID and uses it as the calling party number.
clid restrict	Prevents the calling party number from being presented by CLID.
clid second-number strip	Prevents the second network number from being sent in the CLID information.
isdn global-disconnect	Specifies setting for allowing passage of Release and Release Complete messages over a voice network.
isdn protocol-emulate	Enables emulation of the network side of an ISDN configuration for a PRI Net5 or PRI NTT switch type.
isdn protocol-emulate (dial)	Configures the Layer 2 and Layer 3 port protocol of a BRI voice port or a PRI to emulate NT (network) or TE (user) functionality.
isdn switch-type (BRI)	Specifies the central office switch type on an ISDN BRI.
isdn switch-type (PRI)	Specifies the central office switch type or enables support of QSIG or Q.931 signaling on an ISDN PRI.
session target	Specifies a network-specific address for a dial peer.
signal-end-to-end	Configures R2 transparency using GTD on an R2-based E1 CAS network. (Does not apply to SIP.)
signaling forward (dial-peer)	Specifies tunneling for QSIG, Q.931, H.225, and ISUP messages over a specific dial peer on a SIP or H.323 gateway.

signaling forward (dial peer)

To configure settings for transparent tunneling of Q-signaling (QSIG), Q.931, H.225, and ISDN User Part (ISUP) messages over an individual dial peer that override global settings for a Cisco IOS voice gateway, use the **signaling forward** command in dial peer voice configuration mode. To specify that transparent tunneling behavior on a dial peer be determined by global settings for the gateway, use the **no** form of this command.

Cisco IOS H.323 Dial Peers
signaling forward {**conditional** | **none** | **rawmsg** | **unconditional**}
no signaling forward

Cisco IOS SIP Dial Peers
signaling forward {**none** | **rawmsg** | **unconditional**}
no signaling forward

Syntax Description

conditional	Overrides global settings for the gateway and specifies that tunneling on an H.323 dial peer is determined by the target. (The target is defined using the **session target** command.) This is the default setting for an H.323 dial peer if a global setting is not configured for the gateway. **Note** The **conditional** keyword is not supported on Session Initiation Protocol (SIP) dial peers. Instead, the default setting for SIP dial peers is that no tunneling is configured (**none**).
none	Overrides global settings for the gateway and specifies that the dial peer does not forward Generic Transparency Descriptor (GTD), QSIG, or Q.931 payloads to any endpoint in the network. This is the default setting for a SIP dial peer.
rawmsg	Overrides global settings for the gateway and specifies that the dial peer tunnel QSIG (application-qsig) or Q.931 raw messages (application-Xq931) only, without GTD.
unconditional	Specifies unconditional tunneling and forwards GTD payload along with the QSIG or Q.931 message body even if the attached external route server has modified it. (The gatekeeper sends its own GTD back to itself.)

Command Default

The dial peers use the global setting for transparent tunneling if it is configured for the gateway. If global configuration of the gateway is not specified, the following are the default behaviors for dial peers:

- **conditional** --messages are forwarded according to the target:
  - Non-Registration, Admission, and Status (RAS) targets--only the original payload (without GTD) is forwarded to the H.323 endpoint.
  - All other targets--GTD payload is forwarded along with the message body.

No transparent tunneling of QSIG or Q.931 messages is configured.

Command Modes

Dial peer voice configuration (config-dial-peer)

Command History

Release	Modification
12.2(11)T	This command was introduced on the Cisco AS5350 and Cisco AS5850.
12.4(15)XY	Support was added for passing RELEASE and RELEASE COMPLETE messages end to end over SIP using QSIG tunneling on Cisco IOS voice gateways.
12.4(15)XZ	Support was added for Q.931 tunneling over SIP on Cisco IOS voice gateways and tunneling of both QSIG and Q.931 over SIP was extended to the Cisco Unified Border Element (CUBE). **Note** The CUBE is formerly known as the Cisco IOS Session Border Controller (SBC) or the Cisco Multiservice IP-to-IP Gateway.
12.4(20)T	Support was added for QSIG and Q.931 tunneling over SIP on Cisco IOS voice gateways and the CUBE.

Usage Guidelines

This command is used to configure tunneling behavior for individual dial peers on H.323 and SIP voice gateways. Depending on your specific Cisco router, platform, and network, you can use this command to configure tunneling behavior for various messages, such as QSIG, Q.931, H.225, and ISUP messages. To configure the global setting for a gateway, use the **signaling forward** command in voice service VoIP configuration mode.

For more specific information about controlling tunneling behavior using the **signaling forward** command, see the information included in the following sections:

QSIG and Q.931 Tunneling

Tunneling of QSIG and Q.931 on H.323 gateways is enabled by default for Cisco IOS gateway platforms supporting the **signaling forward** command. For QSIG and Q.931 tunneling on SIP gateways, however, you must configure at least one interface on both an ingress, or originating gateway (OGW), and an egress, or terminating gateway (TGW).

In addition to signaling forward settings, you must specify QSIG or Q.931 as the central office switch type on the ISDN interface for both the OGW and TGW on a SIP or H.323 network. Use the **isdn switch-type** command to enable and specify the switch type:

- For tunneling QSIG messages, specify the **primary-qsig** switch type.
- For tunneling Q.931 messages, specify any ISDN switch type except **primary-qsig** and **primary-dpness**.

Note Cisco IOS SIP gateways do not support the **primary-dpness** switch type for tunneling of Q.931.

Displays QSIG and Q.931 tunneling behavior as determined by gateway voice class and configuration settings.

Table 224: QSIG Tunneling Behavior by Voice Class and Signaling Forward Setting

Signaling Forward Configuration	H.323 Gateway	SIP Gateway
conditional or no specified setting:	Default.	Not supported.

Signaling Forward Configuration	H.323 Gateway	SIP Gateway
session target *non-ras*	Tunnels GTD payload with QSIG or Q.931 message bodies.	No tunneling.
session target ras	Tunnels only QSIG or Q.931 message bodies.	No tunneling.
none	No tunneling.	No tunneling.
rawmsg	Tunnels QSIG or Q.931 message bodies only.	Tunnels QSIG or Q.931 message bodies only.
unconditional	Tunnels GTD payload along with QSIG or Q.931 message bodies.	Tunnels GTD payload along with QSIG or Q.931 message bodies.

SS7 ISUP and H.225 Tunneling over H.323

ISUP defines the protocol and procedures used to configure, manage, and release trunk circuits that carry voice and data calls over the Public Switched Telephone Network (PSTN). ISUP is used for both ISDN and non-ISDN calls and is reconstructed on the basis of the protocol at the egress side of the network, without any concern for the ISDN or ISUP variant on the ingress side of the network.

When you specify that ISDN (H.225) or ISUP information be provided in text format, the information can also be used by applications inside the core H.323 network such as, in a route server, which can use certain ISDN and ISUP information for routing decisions. Additionally, transporting ISUP encapsulated in GTD maintains compatibility with the H.323 protocol.

If the target is a RAS target, for a non-GTD signaling payload, the original payload is forwarded. For a GTD signaling payload, the payload is encapsulated in an admission request (ARQ)/disengage request (DRQ) message and sent to the originating gatekeeper. The gatekeeper conveys the payload to the Gatekeeper Transaction Message Protocol (GKTMP) and external route server for a flexible route decision based upon the ISUP GTD parameters. The gateway then conditionally forwards the GTD payload on the basis of the instruction from the route server.

To tunnel the ISUP GTD, you must configure a dial peer on both the OGW and TGW to encapsulate SS7 ISUP messages in GTD format.

Note If you specify **primary-qsig** as the **isdn switch-type** setting, you must assign network-side functionality (either at the global or dial-peer level) using the **isdn protocol-emulate** command.

Examples

The following example shows unconditional signal forwarding being set on a SIP dial peer (overriding the global setting for the Cisco IOS voice gateway):

```
Router> enable
Router# configure
 terminal
Router(config)# dial-peer
 voice 1
Router(config-dial-peer)# signaling forward unconditional
Router(config-dial-peer)# session protocol sipv2
```

The following example is sample output from the **show running-config** command when a SIP dial peer is configured with unconditional signal forwarding:

```
Router# show running-config
Building configuration...
Current configuration : 2357 bytes
!
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
!
boot-start-marker
no boot startup-test
boot-end-marker
.
.
.
!
dial-peer voice 101 voip
 signaling forward unconditional
 session protocol sipv2
 session target ipv4:9.13.19.114
 incoming called-number 8000
 codec g711ulaw
!
.
```

Note The "session protocol sipv2" in the output indicates that this is a SIP dial peer.

The following example shows unconditional signal forwarding being set on an H.323 dial peer (overriding the global setting for the Cisco IOS voice gateway):

```
Router> enable
Router# configure
 terminal
Router(config)# dial-peer
 voice 1
Router(config-dial-peer)# signaling forward unconditional
```

The following example is sample output from the **show running-config** command when an H.323 dial peer is configured with unconditional signal forwarding:

```
Router# show running-config
Building configuration...
Current configuration : 2357 bytes
!
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
!
boot-start-marker
no boot startup-test
boot-end-marker
.
```

```
.
.
!
dial-peer voice 101 voip
 signaling forward unconditional
 session target ipv4:9.13.19.114
 incoming called-number 8000
 codec g711ulaw
!
.
.
```

Note There is no "session protocol sipv2" in the output, indicating that this is an H.323 dial peer.

Related Commands

clid network-number	Configures a network number in the router for CLID and uses it as the calling party number.
clid restrict	Prevents the calling party number from being presented by CLID.
clid second-number strip	Prevents the second network number from being sent in the CLID information.
isdn global-disconnect	Specifies setting for allowing passage of Release and Release Complete messages over a voice network.
isdn protocol-emulate	Enables emulation of the network side of an ISDN configuration for a PRI Net5 or PRI NTT switch type.
isdn protocol-emulate (dial)	Configures the Layer 2 and Layer 3 port protocol of a BRI voice port or a PRI to emulate NT (network) or TE (user) functionality.
isdn switch-type (BRI)	Specifies the central office switch type on an ISDN BRI.
isdn switch-type (PRI)	Specifies the central office switch type or enables support of QSIG or Q.931 signaling on an ISDN PRI.
session protocol (dial peer)	Specifies a session protocol on a dial peer for calls between local and remote routers using the packet network.
session target	Specifies a network-specific address for a dial peer.
signal-end-to-end	Configures R2 transparency using GTD on an R2-based E1 CAS network. (Does not apply to SIP.)
signaling forward	Specifies tunneling for QSIG, Q.931, H.225, and ISUP messages globally for a SIP or H.323 gateway.

signal-type

To set the signaling type to be used when connecting to a dial peer, use the **signal-type** command in dial-peer configuration mode. To reset to the default, use the **no** form of this command.

signal-type {**cas** | **cept** | **ext-signal** | **transparent**}
no signal-type

Syntax Description

cas	North American EIA-464 channel-associated signaling (robbed bit signaling). If the Digital T1 Packet Voice Trunk Network Module is installed, this option might not be available.
cept	Provides a basic E1 ABCD signaling protocol. Used primarily for E&M interfaces. When used with FXS/FXO interfaces, this protocol is equivalent to MELCAS.
ext -signal	External signaling. The digital signal processor (DSP) does not generate any signaling frames. Use this option when there is an external signaling channel, for example, CCS, or when you need to have a permanent "dumb" voice pipe.
transparent	Selecting this option produces different results depending on whether you are using a digital voice module (DVM) or an analog voice module (AVM). For a DVM: The ABCD signaling bits are copied from or transported through the T1/E1 interface "transparently" without modification or interpretation. This enables the handling of arbitrary or unknown signaling protocols. For an AVM: It is not possible to provide "transparent" behavior without interpreting the signaling information to read and write the correct state to the analog hardware. This option is mapped to be equal to **cas**.

Command Default

cas

Command Modes

Dial-peer configuration (config-dial-peer)

Command History

Release	Modification
12.0(3)XG	This command was introduced on the Cisco 2600, Cisco 3600, and Cisco MC3810.
12.0(4)T	This command was implemented on the Cisco 7200 series.
12.0(7)XK	The **cept** and **transparent** keywords, previously supported only on the Cisco MC3810, are now supported on the Cisco 2600 series, Cisco 3600 series, and 7200 series.
12.1(2)T	This command was integrated into Cisco IOS Release 12.1(2)T.

Usage Guidelines

This command applies to Voice over Frame Relay (VoFR) and Voice over ATM (VoATM) dial peers. It is used with permanent connections only (Cisco trunks and FRF.11 trunks), not with switched calls.

This command is used to inform the local telephony interface of the type of signaling it should expect to receive from the far-end dial peer. To turn signaling off at this dial peer, select the **ext-signal** option. If

signaling is turned off and there are no external signaling channels, a "hot" line exists, enabling this dial peer to connect to anything at the far end.

When you connect an FXS to another FXS, or if you have anything other than an FXS/FXO or E&M/E&M pair, the appropriate signaling type on Cisco 2600 and Cisco 3600 series routers is **ext-signal** (disabled).

If you have a digital E1 connection at the remote end that is running cept/MELCAS signaling and you then trunk that across to an analog port, you should make sure that you configure both ends for the **cept** signal type.

If you have a T1 or E1 connection at both ends and the T1/E1 is running a signaling protocol that is neither EIA-464, or cept/MELCAS, you might want to configure the signal type for the transparent option in order to pass through the signaling.

Examples

The following example disables signaling for VoFR dial peer 200:

```
dial-peer voice 200 vofr
 signal-type ext-signal
 exit
```

Related Commands

Command	Description
codec (dial-peer)	Specifies the voice coder rate of speech for a dial peer.
connection	Specifies the connection mode for a voice port.
destination-pattern	Specifies the telephone number associated with a dial peer.
dtmf-relay	Enables the DSP to generate FRF.11 Annex A frames for a dial peer.
preference	Enables the preferred dial peer to be selected when multiple dial peers within a hunt group are matched for a dial string.
sequence-numbers	Enables the generation of sequence numbers in each frame generated by the DSP.
session protocol	Establishes the VoFR protocol for calls between local and remote routers.
session target	Specifies a network-specific address for a dial peer.

silent-discard untrusted

To discard SIP requests from untrusted sources on an incoming SIP trunk, use **silent-discard untrusted** command in "voice service voip >> sip" configuration mode. To disable, use **no** form of this command.

silent-discard untrusted
no silent-discard untrusted

Command Default

This command is enabled by default. SIP requests from untrusted sources are discarded.

Command Modes

voice service voip >> sip

Command History

Release	Modification
Cisco IOS XE 3.10S Cisco IOS 15.3(3)M	This command was introduced.
Cisco IOS XE Cupertino 17.7.1a	Introduced support for YANG models.

Usage Guidelines

Use this command to enable TDoS attack mitigation.

Example

The following example shows how to configure CUBE to discard SIP requests from untrusted sources on an incoming SIP trunk:

```
Device> enable
Device# configure terminal
Device(config)# voice service voip
Device(conf-voi-serv)# ip address trusted authenticate
Device(conf-voi-serv)# allow-connections sip to sip
Device(conf-voi-serv)# sip
Device(conf-serv-sip)# silent-discard untrusted
```

silent-fax

To configure the voice dial peer for a Type 2 silent fax machine, use the **silent-fax** command in dial peer configuration mode. To disable a silent fax call to any POTS ports, use the **no** form of this command.

silent-fax
no silent-fax

Syntax Description

This command has no arguments or keywords.

Command Default

Silent fax is not configured.

Command Modes

Dial peer configuration (config-dial-peer)

Command History

Release	Modification
12.2(8)T	This command was introduced on the Cisco 803, Cisco 804, and Cisco 813.

Usage Guidelines

Use this command to configure the router to send a no ring alert tone to a Type 2 silent fax machine that is connected to any of the POTS ports. To check the status of the silent-fax configuration, use the **show running-config** command.

Examples

The following example shows that the **silent-fax** command has been configured on POTS port 1 but not on POTS port 2.

```
dial-peer voice 1 pots
 destination-pattern 5551111
 port 1
 no call-waiting
 ring 0
 volume 4
 caller-number 3334444 ring 1
 subaddress 20
 silent-fax
dial-peer voice 2 pots
 destination-pattern 5552222
 port 2
 no call-waiting
 ring 0
 volume 2
 caller-number 3214567 ring 2
 subaddress 10
```

Related Commands

Command	Description
show running-config	Displays the contents of the currently running configuration file or the configuration for a specific class map, interface, map class, policy map, or VC class.

sip

To enter the Session Initiation Protocol (SIP) configuration mode, use the **sip** command in voice-service VoIP configuration mode.

sip

Syntax Description

This command has no arguments or keywords.

Command Default

No default behavior or values.

Command Modes

Voice-service VoIP configuration (config-voi-srv)

Command History

Release	Modification
12.2(2)XB	This command was introduced on the Cisco 2600 series, Cisco 3600 series, Cisco 7200 series, Cisco AS5300, Cisco AS5350, and Cisco AS5400 platforms.
12.2(2)XB2	This command was implemented on the Cisco AS5850 platform.
12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T and support was added for the Cisco 3700 series. Cisco AS5300, Cisco AS5350, Cisco AS5850, and Cisco AS5400 platforms were not supported in this release.
12.2(11)T	Support was added for the Cisco AS5300, Cisco AS5350, Cisco AS5400, and Cisco AS5850 platforms.
12.2(33)XNE	This command was integrated into Cisco IOS Release 12.2(33)XNE.
Cisco IOS XE Amsterdam 17.2.1r	Introduced support for YANG models.

Usage Guidelines

From the voice-service VoIPconfiguration mode, the **sip** command enables you to enter SIP configuration mode. From this mode, several SIP commands are available, such as **bind**, **session transport**, and **url**.

Examples

The following example illustrates entering SIP configuration mode and then setting the **bind** command on the SIP network:

```
Router(config)# voice service voip
Router(config-voi-srv)# sip
Router(conf-serv-sip)# bind control source-interface FastEthernet 0
```

Related Commands

Command	Description
voice service voip	Enters the voice-service configuration mode.

Command	Description
session transport	Configures the voice dial peer to use Transmission Control Protocol (TCP) or User Datagram Protocol (UDP) as the underlying transport layer protocol for SIP messages.

sip-header

To specify the Session Initiation Protocol (SIP) header to be sent to the peer call leg, use the **sip-header** command in voice class configuration mode. To disable the configuration, use the **no** form of this command.

sip-header {**sip-req-uri***header-name*}
no sip-header {**sip-req-uri***header-name*}

Syntax Description

sip-req-uri	Configures Cisco Unified Border Element (UBE) to send a SIP request Uniform Resource Identifier (URI) to the peer call leg.
header-name	Name of the header to be sent to the peer call leg.

Command Default

SIP header is not sent to the peer call leg.

Command Modes

Voice class configuration (config-class)

Command History

Release	Modification
15.1(3)T	This command was introduced.

Usage Guidelines

Use the **sip-header** command to configure Cisco UBE to pass the unsupported parameters present in a mandatory header from one peer call leg to another of a Cisco UBE.

Examples

The following example shows how to configure Cisco UBE to send a "From" header to the peer call leg:

```
Router(config)# voice class sip-copylist 2
Router(config-class)# sip-header From
```

Related Commands

Command	Description
voice class sip-copylist	Configures a list of entities to be sent to a peer call leg and enters voice class configuration mode.

sip-header SIP-StatusLine

To specify that the Session Initiation Protocol (SIP) status line header must be sent to the peer call leg, use the **sip-header SIP-StatusLine** command in voice class configuration mode. To disable this configuration, use the **no** form of the command.

sip-header SIP-StatusLine
no sip-header SIP-StatusLine

Syntax Description

This command has no keywords or arguments.

Command Default

The SIP status line header is not sent to the peer call leg.

Command Modes

Voice class configuration (config-class)

Command History

Release	Modification
15.4(1)T	This command was introduced.

Usage Guidelines

A list of entities to be sent to the peer call leg using the **voice class sip-copylist** command must be configured before specifying that the SIP status line header must be sent to the peer call leg using the **sip-header SIP-StatusLine** command.

Example

The following example shows how to specify that the SIP status line header must be sent to the peer call leg using the **sip-header SIP-StatusLine** command:

```
Device> enable
Device# configure terminal
Device(config)# voice class sip-copylist 1
Device(config-class)# sip-header SIP-StatusLine
```

Related Commands

Command	Description
voice class sip-copylist	Configures a list of entities to be sent to the peer call leg.

sip-server

To configure a network address for the Session Initiation Protocol (SIP) server interface, use the **sip-server** command in SIP user-agent configuration mode or voice class tenant configuration mode. To remove a network address configured for SIP, use the **no** form of this command.

sip-server {**dns:***host-name* | **ipv4:***ipv4-address[:port-num]* | **ipv6:***ipv6-address*[*:port-num*]}
no sip-server

Syntax Description

dns:*host-name*	Sets the global SIP server interface to a Domain Name System (DNS) hostname. If you specify a hostname, the default DNS defined by the ip name-server command is used. Hostname is optional. Valid DNS hostname in the following format: name.gateway.xyz.
ipv4:*ipv4-address*	Sets the global SIP server interface to an IPv4 address. A valid IPv4 address takes the following format: xxx.xxx.xxx.xxx.
ipv6:*ipv6-address*	Sets the global SIP server interface to an IPv6 address. You must enter brackets around the IPv6 address.
:*port-num*	(Optional) Port number for the SIP server.

Command Default

No network address is configured.

Command Modes

SIP user-agent configuration (config-sip-ua)

Voice class tenant configuration (config-class)

Command History

Release	Modification
12.1(1)T	This command was introduced on the Cisco 2600 series, Cisco 3600 series, and Cisco AS5300.
12.2(2)XA	This command was implemented on the Cisco AS5350 and Cisco AS5400.
12.2(2)XB1	This command was implemented on the Cisco AS5850.
12.2(8)T	This command was implemented on the Cisco 7200 series. Support for the Cisco AS5300, Cisco AS5350, Cisco AS5400, and Cisco AS5850 was not included in this release.
12.2(11)T	This command was integrated into Cisco IOS Release 12.2(11)T. This command was implemented on the Cisco AS5300, Cisco AS5350, Cisco AS5400, and Cisco AS5850.
12.4(22)T	Support for IPv6 was added.
15.6(2)T and IOS XE Denali 16.3.1	This command is now available under voice class tenants.
Cisco IOS XE Cupertino 17.7.1a	Introduced support for YANG models.

Usage Guidelines

If you use this command, you can also use the **session target sip-server** command on each dial peer instead of repeatedly entering the SIP server interface address for each dial peer. Configuring a SIP server as a session target is useful if a Cisco SIP proxy server (SPS) is present in the network. With an SPS, you can configure the SIP server option and have the interested dial peers use the SPS by default.

To reset this command to a null value, use the **default** command.

To configure an IPv6 address, the user must enter brackets [ ] around the IPv6 address.

Examples

The following example, beginning in global configuration mode, sets the global SIP server interface to the DNS hostname "3660-2.sip.com." If you also use the **session target sip server** command , you need not set the DNS hostname for each individual dial peer.

```
sip-ua
 sip-server dns:3660-2.sip.com
dial-peer voice 29 voip
 session target sip-server
```

The following example sets the global SIP server interface to an IPv4 address:

```
sip-ua
 sip-server ipv4:10.0.2.254
```

The following example sets the global SIP server interface to an IPv6 address. Note that brackets were entered around the IPv6 address:

```
sip-ua
 sip-server ipv6:[2001:0DB8:0:0:8:800:200C:417A]
```

Related Commands

Command	Description
default	Enables a default aggregation cache.
ip name-server	Specifies the address of one or more name servers to use for name and address resolution.
session target (VoIP dial peer)	Specifies a network-specific address for a dial peer.
session target sip-server	Instructs the dial peer session target to use the global SIP server.
sip-ua	Enters SIP user-agent configuration mode in order to configure the SIP user agent.

sip-ua

To enable Session Initiation Protocol (SIP) user-agent configuration commands, use the **sip-ua** command in global configuration mode. To reset all SIP user-agent configuration commands to their default values, use the **no** form of this command.

sip-ua
no sip-ua

Syntax Description

This command has no arguments or keywords.

Command Default

If this command is not enabled, no SIP user-agent configuration commands can be entered.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.1(1)T	This command was introduced on the following platforms: Cisco 2600 series, Cisco 3600 series, and Cisco AS5300.
12.2(2)XA	This command was implemented on the Cisco AS5350 and Cisco AS5400.
12.2(2)XB1	This command was implemented on the Cisco AS5850.
12.2(8)T	This command was implemented on the Cisco 7200 series. Support for the Cisco AS5300, Cisco AS5350, Cisco AS5400, and Cisco AS5850 was not included.
12.2(11)T	This command was integrated into Cisco IOS Release 12.2(11)T. Support for Cisco AS5300, Cisco AS5350, Cisco AS5400, and Cisco AS5850 was included.
15.1(2)T	This command was modified. The **connection-reuse** SIP user-agent configuration mode command was added to the **sip-ua** command.
15.2(4)M	This command was modified. The **via-port** option was added to the **connection-reuse** SIP user-agent configuration mode command.
Cisco IOS XE Amsterdam 17.2.1r	Introduced support for YANG models.

Usage Guidelines

Use this command to enter SIP user-agent configuration mode. The table below lists the SIP user-agent configuration mode commands.

Table 225: SIP User-Agent Configuration Mode Commands

Command	Description
connection-reuse	Uses the listener port for sending requests over the UDP. The **via-port** option sends SIP responses to the port present in the Via header instead of the source port on which the request was received. Note that the **connection-reuse** command is a SIP user-agent configuration mode command.
exit	Exits SIP user-agent configuration mode.
inband-alerting	This command is no longer supported as of Cisco IOS Release 12.2 because the gateway handles remote or local ringback on the basis of SIP messaging.
max-forwards	Specifies the maximum number of hops for a request.
retry	Configures the SIP signaling timers for retry attempts.
sip-server	Configures the SIP server interface.
timers	Configures the SIP signaling timers.
transport	Enables or disables a SIP user agent transport for the TCP or UDP that the protocol SIP user agents listen for on port 5060 (default).

Examples

The following example shows how to enter SIP user-agent configuration mode and configure the SIP user agent:

```
Device> enable
Device# configure terminal
Device(config)# sip-ua
Device(config-sip-ua)# retry invite 2
Device(config-sip-ua)# retry response 2
Device(config-sip-ua)# retry bye 2
Device(config-sip-ua)# retry cancel 2
Device(config-sip-ua)# sip-server ipv4:192.0.2.1
Device(config-sip-ua)# timers invite-wait-100 500
Device(config-sip-ua)# exit
Device#
```

Related Commands

Command	Description
exit	Exits SIP user-agent configuration mode.
max-forwards	Specifies the maximum number of hops for a request.
retry	Configures the retry attempts for SIP messages.
show sip-ua	Displays statistics for SIP retries, timers, and current listener status.
sip-server	Configures the SIP server interface.
timers	Configures the SIP signaling timers.

Command	Description
transport	Configures the SIP user agent (gateway) for SIP signaling messages on inbound calls through the SIP TCP or UDP socket.

sni send (voice class)

To enable Server Name Indication (SNI), and associate it to a TLS profile, use the command **sni send** in voice class configuration mode. To disable Server Name Indication, use the **no** form of this command.

sni send
no sni send

Syntax Description

This command has no arguments or keywords.

Command Default

Server Name Indication (SNI) is disabled.

Command Modes

Voice class configuration (config-class)

Command History

Release	Modification
Cisco IOS XE Amsterdam 17.3.1a	This command was introduced under voice class configuration mode.

Usage Guidelines

Server Name Indication (SNI) functionality is associated to a TLS profile through the command **voice class tls-profile** *tag*. The *tag* associates the SNI functionality to the command **crypto signaling**.

sni send enables Server Name Indication (SNI), a TLS extension that allows a TLS client to indicate the name of the server that it is trying connect during the initial TLS handshake process. Only the fully qualified DNS hostname of the server is sent in the client hello. SNI does not support IPv4 and IPv6 addresses in the client hello extension. After receiving a "hello" with the server name from the TLS client, the server uses appropriate certificate in the subsequent TLS handshake process. Only TLS1.2 version is supported with SNI.

Examples

The following example illustrates how to create a voice class tls-profile and associate SNI functionality that is required during the TLS handshake:

```
Router(config)#voice class tls-profile 2
Router(config-class)#sni send
```

Related Commands

Command	Description
voice class tls-profile	Provides sub-options to configure the commands that are required for a TLS session.
crypto signaling	Identifies the trustpoint or the **tls-profile** *tag* that is used during the TLS handshake process.

snmp enable peer-trap dscp-profile

To enable differentiated services code point (DSCP) profile violation traps at the dial peer level, use the **snmp enable peer-trap dscp-profile** command in dial peer voice configuration mode. To disable the configuration, use the **no** form of this command.

snmp enable peer-trap dscp-profile
no snmp enable peer-trap dscp-profile

Syntax Description

This command has no arguments or keywords.

Command Default

DSCP profile violation traps are not enabled.

Command Modes

Dial peer voice configuration (config-dial-peer)

Command History

Release	Modification
15.2(2)T	This command was introduced.

Usage Guidelines

If you enable the DSCP profile violation trap both at the global level and the dial peer level, the dial peer configuration takes precedence over the global level configuration.

Examples

The following example shows how to enable DSCP profile violation traps for a dial peer:

```
Router> enable
Router# configure terminal
Router(config)# dial-peer voice 4 voip
Router(config-dial-peer)# snmp enable peer-trap dscp-profile
Router(config-dial-peer)# end
```

Related Commands

Command	Description
snmp-server enable traps voice dscp-profile	Enables DSCP profile violation traps at the global level.

snmp enable peer-trap poor-qov

To generate poor-quality-of-voice notifications for applicable calls associated with VoIP dial peers, use the **snmp enable peer-trap poor-qov**command in dial peer configuration mode. To disable notification, use the **no** form of this command.

snmp enable peer-trap poor-qov
no snmp enable peer-trap poor-qov

Syntax Description

This command has no arguments or keywords.

Command Default

Disabled

Command Modes

Dial peer configuration (config-dial-peer)

Command History

Release	Modification
11.3(1)T	This command was introduced on the Cisco 3600 series.

Usage Guidelines

Use this command to generate poor-quality-of-voice notification for applicable calls associated with a dial peer. If you have a Simple Network Management Protocol (SNMP) manager that uses SNMP messages when voice quality drops, you might want to enable this command. Otherwise, you should disable this command to reduce unnecessary network traffic.

Examples

The following example enables poor-quality-of-voice notification for calls associated with VoIP dial peer 10:

```
dial-peer voice 10 voip
 snmp enable peer-trap poor-qov
```

Related Commands

Command	Description
snmp -server enable traps	Enables a router to send SNMP traps and information.
snmp trap link -status	Enables SNMP trap messages to be generated when a specific port is brought up or down.

snmp-server enable traps voice (DSCP profile)

To enable Simple Network Management Protocol (SNMP) voice notifications, use the **snmp-server enable traps voice** command in global configuration mode. To disable the voice notifications, use the **no** form of this command.

snmp-server enable traps voice [**dscp-profile**] [**fallback**] [**high-ds0-util**] [**low-ds0-util**] [**media-policy**] [**poor-qov**]
no snmp-server enable traps voice dscp-profile [**fallback**] [**high-ds0-util**] [**low-ds0-util**] [**media-policy**] [**poor-qov**]

Syntax Description

dscp-profile	(Optional) Enables differentiated services code point (DSCP) voice traps.
fallback	(Optional) Enables SNMP fallback voice traps.
high-ds0-util	(Optional) Enables SNMP high utilization of Digital Signal 0 (DS0) traps.
low-ds0-util	(Optional) Enables SNMP low utilization of DS0 traps.
media-policy	(Optional) Enables SNMP media policy voice traps.
poor-qov	(Optional) Enables SNMP poor quality of voice traps.

Command Default

SNMP DSCP profile voice notifications are disabled.

Command Modes

Global configuration (config)

Command History

Release	Modification
15.2(2)T	This command was introduced.

Usage Guidelines

Use the **snmp-server enable traps voice** command to enable SNMP traps for DSCP marking and policing.

Examples

The following example shows how to enable SNMP media policy voice notifications:

```
Router> enable
Router# configure terminal
Router(config)# snmp-server enable traps voice dscp-profile media-policy
```

Related Commands

Command	Description
dscp media	Specifies the RPH to DSCP mapping.
violation	Specifies the action that needs to be performed on any violation in the DSCP policy.

soft-offhook

To enable stepped off-hook resistance during seizure, use the **soft-offhook** command in voice-port (FXO) configuration mode. To disable this command, use the **no** form of this command.

soft-offhook
no soft-offhook

Syntax Description

This command has no arguments or keywords.

Command Default

This command is disabled by default, which means there is no stepped off-hook resistance during seizure.

Command Modes

Voice-port (FXO) configuration (config-voiceport)

Command History

Release	Modification
12.4(3f) 12.4(4)T4	This command was introduced.

Usage Guidelines

An off-hook indication into a far-end ringing cadence ON condition can occur during glare conditions (outgoing seizure occurring at the same time as an incoming ring). This condition can also occur when the interface configuration includes the **connection plar-opx** command. If the **connection plar-opx** command is not configured, the FXO software waits for a ringing cadence to transition from ON to OFF prior to transitioning to the off-hook condition. (Glare can be minimized by configuring ground-start signaling.)

When the **soft-offhook** command is entered, the FXO hookswitch off-hook resistance is initially set to a midresistance value for outgoing or incoming seizure. This resistance limits the ringing current that occurs during seizure into ringing signals prior to far-end ring-trip. When ringing is no longer detected, hookswitch resistance is returned to its normal lower value. This prevents damage to the FXO line interface that may occur in locations with short loops and conventional ringing sources with low output impedance ringing sources that have the potential to deliver high current.

The **soft-offhook** command applies to the following FXO interface cards (which use the 3050i chipset):

- EM-HDA-3FXS/4FXO (EVM-HD-8FXS/DID, FXO ports only)
- EM-HDA-6FXO (on EVM-HD-8FXS/DID)
- EM2-HDA-4FXO (NM-HDA-4FXS network module only)
- VIC2-4FXO, VIC2-2FXO

Examples

The following example shows a sample configuration session to enable stepped off-hook resistance during seizure on voice port 1/0/0 on a Cisco 3725 router:

```
Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# voice-port 1/0/0
Router(config-voiceport)# soft-offhook
Router(config-voiceport)# shutdown
Router(config-voiceport)#
Nov  3 11:08:53.313 EST: %LINK-3-UPDOWN: Interface Foreign Exchange Office 1/0/0, changed
```

```
state to Administrative Shutdown
Router(config-voiceport)# no shutdown

Router(config-voiceport)#
Nov  3 11:08:58.290 EST: %LINK-3-UPDOWN: Interface Foreign Exchange Office 1/0/0, changed
state to up
Router(config-voiceport)# ^Z

Router#
Nov  3 11:09:01.086 EST: %SYS-5-CONFIG_I: Configured from console by console
Router#
```

Related Commands

Command	Description
connection plar-opx	Specifies the connection mode for a voice port as PLAR-OPX.
voice-port	Enters voice-port configuration mode.

source-address (uc-wsapi)

To specify the source IP address or hostname for the Cisco Unified Communication IOS services in the NotifyProviderStatus message, use the **source-address** command in uc wsapi configuration mode. To disable the router from sending NotifyProviderStatus message, use the **no** form of this command.

source-address *ip-address*
no source-address

Syntax Description

ip-address	The IP address identified as the source address by the service provider in the NotifyProviderStatus message.

Command Default

No IP address

Command Modes

uc wsapi

Command History

Release	Modification
15.2(2)T	This command was introduced.

Usage Guidelines

This command enables the service provider on the router to send messages to the application via the NotifyProvicerStatus message.

Examples

The following example shows how to set the IP source address and port.

```
Router(config)# uc wsapi
Router(config-register-global)# source-address 172.1.12.13
```

Related Commands

Command	Description
provider	Enables a provider service.
remote-url	Specifies the URL of the application.
uc wsapi	Enters Cisco Unified Communication IOS services configuration mode.

source carrier-id

To configure debug filtering for the source carrier ID, use the **source carrier-id** command in call filter match list configuration mode. To disable, use the **no** form of this command.

source carrier-id *string*
no source carrier-id *string*

Syntax Description

string	Alphanumeric identifier for the carrier ID.

Command Default

No default behavior or values

Command Modes

Call filter match list configuration

Command History

Release	Modification
12.3(4)T	This command was introduced.

Examples

The following example shows the voice call debug filter set to match source carrier ID 4321:

```
call filter match-list 1 voice
 source carrier-id 4321
```

Related Commands

Command	Description
call filter match-list voice	Creates a call filter match list for debugging voice calls.
debug condition match-list	Run a filtered debug on a voice call.
show call filter match-list	Displays call filter match lists.
source trunk-group-label	Configures debug filtering for a source trunk group.
target carrier-id	Configures debug filtering for the target carrier ID.
target trunk-group-label	Configures debug filtering for a target trunk group.

source filter

To filter Real-time Transport Protocol (RTP) packets with a source IP address and port number that are different from the one negotiated through Session Initiation Protocol (SIP) signaling, use the **source filter** command in voice service SIP configuration mode. To disable filtering, use the **no** form of this command.

source filter
no source filter

Command Default

RTP source filtering is disabled.

Command Modes

Voice service SIP configuration (conf-serv-sip)

Command History

Release	Modification
12.4(6)T	This command was introduced.

Usage Guidelines

Public Switched Telephone Network (PSTN) callers may experience crosstalk when the SIP IOS gateway receives an invalid RTP stream destined to the same IP address and port of an active call. The invalid stream has a different source IP address and port than the one negotiated using SIP Session Description Protocol (SDP). The Digital Signal Processor (DSP) within the gateway mixes both the valid and invalid RTP streams and plays it to the PSTN caller. Use the **source filter** command when you want to filter RTP packets with a source IP address and port number that are different from the one negotiated through SIP signaling.

Examples

The following example shows how to filter RTP packets:

```
Device> enable
Device# configure terminal
Device(config)# voice service voip
Device(conf-voi-serv)# sip
Device(conf-serv-sip)# source filter
```

Related Commands

Command	Description
sip	Enters SIP configuration mode.
voice service voip	Specifies the voice-encapsulation type and enters voice service configuration mode.

source-ip (media-profile)

To configure the local source IP address of a WebSocket connection in CUBE, use the **source-ip** command in media profile configuration mode. To remove the configuration, use the **no** form of this command.

source-ip *ip-address*
no source-ip *ip-address*

Syntax Description

ip-address	IP address of the interface to bind with the WebSocket.

Command Default

Disabled by default.

Command Modes

Media Profile configuration mode (cfg-mediaprofile)

Command History

Release	Modification
Cisco IOS XE Bengaluru 17.6.1a	This command was introduced on Cisco Unified Border Element.

Usage Guidelines

A CUBE router can have single or multiple interfaces configured on it. In either case, you must specify the IP address of the interface to bind it with the socket in a WebSocket connection. Use the **source-ip** command in media profile configuration mode to bind the router interface with the socket. The **source-ip** *ip-address* configuration has preference over **http client source interface GigabitEthernet** configuration. If you do not configure **source-ip** , CUBE binds to a suitable IP address on the local interface by default.

Examples

The following is a sample configuration for **source-ip (media-profile)** in CUBE:

```
csr(cfg-mediaprofile)#source-ip ?
ip-address Enter the source IP address

csr(cfg-mediaprofile)#source-ip 10.64.86.70
```

Related Commands

Command	Description
media profile stream-service	Enables stream service on CUBE.
connection (media-profile)	Configures idle timeout and call threshold for a media profile.
proxy (media-profile)	Configures IP address or hostname of proxy in media profile.
description (media-profile)	Specifies a description for the media profile.
media class	Applies the media class at the dial peer level.

source trunk-group-label

To configure debug filtering for a source trunk group, use the **source trunk-group-label** command in call filter match list configuration mode. To disable, use the **no** form of this command.

source trunk-group-label *group_number*
no source trunk-group-label *group_number*

Syntax Description

group_number	A value from 0 to 23 that identifies the trunk group.

Command Default

No default behavior or values

Command Modes

Call filter match list configuration

Command History

Release	Modification
12.3(4)T	This command was introduced.

Examples

The following example shows the voice call debug filter set to match source trunk group 21:

```
call filter match-list 1 voice
 source trunk-group-label 21
```

Related Commands

Command	Description
call filter match-list voice	Creates a call filter match list for debugging voice calls.
debug condition match-list	Runs a filtered debug on a voice call.
show call filter match-list	Displays call filter match lists.
source carrier-id	Configures debug filtering for the source carrier ID.
target carrier-id	Configures debug filtering for the target carrier ID.
target trunk-group-label	Configures debug filtering for a target trunk group.

speed dial

To designate a range of digits for SCCP telephony control (STC) application feature speed-dial codes, use the **speed dial** command in STC application feature speed-dial configuration mode. To return the range to its default, use the **no** form of this command.

speed dial from *digit* **to** *digit*
no speed dial

Syntax Description

from *digit*	Starting number for the range of speed-dial codes. Range is 0 to 9 for one-digit codes; 00 to 99 for two-digit codes. Default is 1 for one-digit codes; 01 for two-digit codes. **Note** Range depends on the number of digits set with the **digit** command.
to *digit*	Ending number for the range of speed-dial codes. Range is 0 to 9 for one-digit codes; 00 to 99 for two-digit codes. Default is 9 for one-digit codes; 99 for two-digit codes. **Note** Range depends on the number of digits set with the **digit** command.

Command Default

The default speed-dial codes are 1 to 9 for one-digit codes; 01 to 99 for two-digit codes.

Command Modes

STC application feature speed-dial configuration

Command History

Release	Modification
12.4(2)T	This command was introduced.
12.4(6)T	The *digit* argument was modified to allow two-digit codes.

Usage Guidelines

This command is used with the STC application, which enables features on analog FXS endpoints that use Skinny Client Control Protocol (SCCP) for call control.

Use this command to set the range of speed-dial codes only if you want to change the range from its default. The **digit** command determines whether speed-dial codes are one-digit or two-digit.

A maximum of nine one-digit or 99 two-digit speed-dial codes are supported. If you set the starting number to 0, the highest number you can set for the ending number is 8 for one-digit codes, or 98 for two-digit codes.

Note that the actual telephone numbers that are speed dialed are stored on Cisco CallManager or the Cisco CallManager Express system. The speed-dial codes that you set with this command are mapped to speed-dial positions on the call-control device. For example, if you set the starting number to 2 and the ending number to 7, the system maps 2 to speed-dial 1 and maps 7 to speed-dial 6.

You can enter numbers in this command in ascending or descending order. For example, the following commands are both valid:

```
Router(stcapp-fsd)# speed dial from 2 to 7
Router(stcapp-fsd)# speed dial from 7 to 2
```

To use the speed-dial feature on a phone, dial the STC application feature speed-dial (FSD) prefix and one of the speed-dial codes that has been configured with this command (or the default if this command was not used). For example, if the FSD prefix is * (the default) and the speed-dial codes are 1 to 9 (the default), dial *3 to dial the telephone number stored with speed-dial 3.

This command resets to its default range if you modify the value of the **digit** command. For example, if you set the **digit** command to 2, then change the **digit** command back to its default of 1, the speed-dial codes are reset to 1 to 9.

If the **digit** command is set to 2 and you configure a single-digit speed-dial code, the system converts the speed-dial code to two digits. For example, if you enter the range 1 to 5 in a two-digit configuration, the system converts the speed-dial codes to 11 to 15.

If you set any of the FSD codes in this range to a value that is already in use for another FSD code, you receive a warning message. If you configure a duplicate code, the system implements the first matching feature in the order of precedence shown in the output of the **show stcapp feature codes** command.

The **show running-config** command displays nondefault FSD codes only. The **show stcapp feature codes** command displays all FSD codes.

Examples

The following example sets an FSD code prefix of two pound signs (##) and a speed-dial code range of 2 to 7. After these values are configured, a phone user presses ##2 to dial the number that is stored with speed-dial 1 on the call-control system (Cisco CallManager or Cisco CallManager Express).

```
Router(config)# stcapp feature speed-dial
Router(stcapp-fsd)# prefix ##
Router(stcapp-fsd)# speed dial from 2 to 7
Router(stcapp-fsd)# exit
```

The following example shows how the speed-dial range that is set in the example above is mapped to the speed-dial positions on the call-control system. Note that the range from 2 to 7 is mapped to speed-dial 1 to 6.

```
Router# show stcapp feature codes
.
.
.
  stcapp feature speed-dial
    prefix ##
    redial ###
    speeddial number of digit(s) 1
    voicemail ##0
    speeddial1 ##2
    speeddial2 ##3
    speeddial3 ##4
    speeddial4 ##5
    speeddial5 ##6
    speeddial6 ##7
```

The following example sets a FSD code prefix of two asterisks (**) and a speed-dial code range of 12 to 17.

```
Router(config)# stcapp feature speed-dial
Router(stcapp-fsd)# prefix **
Router(stcapp-fsd)# digit 2
Router(stcapp-fsd)# speed dial from 12 to 17
Router(stcapp-fsd)# exit
```

Related Commands

Command	Description
digit	Designates the number of digits for STC application feature speed-dial codes.
prefix (stcapp-fsd)	Designates a prefix to precede the dialing of an STC application feature speed-dial code.
redial	Designates an STC application feature speed-dial code to dial again the last number that was dialed.
show running-config	Displays current nondefault configuration settings.
show stcapp feature codes	Displays configured and default STC application feature access codes.
stcapp feature speed-dial	Enters STC application feature speed-dial configuration mode to set feature speed-dial codes.
voicemail (stcapp-fsd)	Designates an STC application feature speed-dial code to dial the voice-mail number.

srtp (dial peer)

To specify that Secure Real-Time Transport Protocol (SRTP) be used to enable secure calls for a specific VoIP dial peer, to enable fallback, and to override global SRTP configuration, use the **srtp** command in dial peer voice configuration mode. To disable secure calls, to disable fallback, and to override global SRTP configuration, use the **no** form of this command.

srtp [**fallback** | **pass-thru]** | **system**]
no srtp [**fallback** | **pass-thru]** | **system**]

Syntax Description

fallback	(Optional) Enables specific dial peer calls to fall back to nonsecure mode.
pass-thru	(Optional) Enables transparent passthrough of all crypto suites (supported and unsupported).
system	(Optional) Enables the global SRTP configuration that was set using the **srtp** command in voice service voip configuration mode. This is the default if the **srtp** command is enabled in dial peer voice configuration mode.

Command Default

Global SRTP configuration set in voice service voip configuration mode is enabled.

Command Modes

Dial peer voice configuration (config-dial-peer)

Command History

Release	Modification
12.4(6)T1	This command was introduced.
15.6(1)T and 3.17S	This command was modified to include keyword: **pass-thru**.
Cisco IOS XE Cupertino 17.7.1a	Introduced support for YANG models.

Usage Guidelines

You can enable secure calls using the **srtp** command either at the dial peer level, or at the global level. The **srtp** command in dial peer voice mode configures call security at the dial-peer level and takes precedence over the global **srtp** command. Use the **srtp** command in dial peer voice configuration mode to enable secure calls for a specific dial peer. Use the **no** form of this command to disable secure calls.

Use the **srtp fallback** command to enable secure calls and allow calls to fallback to nonsecure mode for a specific dial peer. This security policy applies to all calls going through the dial peer and is not configurable on a per-call basis. Using the **srtp fallback** command to configure call fallback at the dial-peer level takes precedence over the global **srtp fallback** command. The **no** form of this command disables SRTP and fallback. If you disallow fallback using the **no srtp fallback** command, a call cannot fall back to nonsecure mode.

To enable the transparent passthrough of all crypto suites for a specific dial peer, use the **srtp pass-thru** command in dial-peer voice configuration mode. If SRTP pass-thru feature is enabled, media interworking will not be supported.

Note Ensure that you have symmetric configuration on both the incoming and outgoing dial-peers to avoid media-related issues.

Use the **srtp system**command to apply global level security settings to dial peers.

Examples

The following example enables secure calls and disallows fallback for a specific dial peer:

```
Router(config-dial-peer)# srtp
```

The following example enables secure calls and allows call fallback to nonsecure mode:

```
Router(config-dial-peer)# srtp fallback
```

The following example enables the transparent passthrough of crypto suites:

```
Router(config-dial-peer)# srtp pass-thru
```

The following example defaults call security to global level SRTP behavior:

```
Router(config-dial-peer)# srtp system
```

Related Commands

Command	Description
srtp (voice)	Enables secure calls globally in voice service voip configuration mode.
srtp fallback (voice)	Enables SRTP and fallback globally.

srtp (voice)

To specify that Secure Real-Time Transport Protocol (SRTP) be used to enable secure calls and call fallback, use the **srtp** command in the global VoIP configuration mode. To disable secure calls and disallow fallback, use the **no** form of this command.

srtp [fallback | pass-thru]
no srtp [fallback | pass-thru]

Syntax Description

fallback	(Optional) Enables call fallback to nonsecure mode.
pass-thru	(Optional) Enables transparent passthrough of all crypto suites (supported and unsupported).

Command Default

Voice call security and fallback are disabled.

Command Modes

Voice service configuration (config-voi-serv)

Dial-peer voice configuration mode (config-dial-peer)

Command History

Release	Modification
12.4(6)T1	This command was introduced.
15.6(1)T and 3.17S	This command was modified to include keyword: **pass-thru**.
Cisco IOS XE Cupertino 17.7.1a	Introduced support for YANG models.

Usage Guidelines

Use the **srtp** command in voice service voip configuration mode to globally enable secure calls using SRTP media authentication and encryption. This security policy applies to all calls going through the gateway and is not configurable on a per-call basis. To enable secure calls for a specific dial peer, use the **srtp** command in dial-peer voice configuration mode. Using the **srtp** command to configure call security at the dial-peer level takes precedence over the global **srtp** command.

Use the **srtp fallback** command to globally enable secure calls and allow calls to fall back to RTP (nonsecure) mode. This security policy applies to all calls going through the gateway and is not configurable on a per-call basis. To enable secure calls for a specific dial peer, use the **srtp** command in dial-peer voice configuration mode. Using the **srtp fallback** command in dial-peer voice configuration mode to configure call security takes precedence over the **srtp fallback** global command in voice service voip configuration mode. If you use the **no srtp fallback** command, fallback from SRTP to RTP (secure to nonsecure) is disallowed.

Use the **srtp pass-thru** to globally enable the transparent passthrough of all (supported and unsupported) crypto suites. To enable the transparent passthrough of all crypto suites for a specific dial peer, use the **srtp pass-thru** command in dial-peer voice configuration mode. If SRTP pass-thru feature is enabled, media interworking will not be supported.



Note Ensure that you have symmetric configuration on both the incoming and outgoing dial-peers to avoid media-related issues.

Examples

The following example enables secure calls:

```
Router(config-voi-serv)# srtp
```

The following example enables call fallback to nonsecure mode:

```
Router(config-voi-serv)# srtp fallback
```

The following example enables the transparent passthrough of crypto suites:

```
Router(config-voi-serv)# srtp pass-thru
```

Related Commands

Command	Description
srtp (dial-peer)	Enables secure calls on an individual dial peer.
srtp fallback (dial-peer)	Enables call fallback to RTP (nonsecure) mode on an individual dial peer.
srtp fallback (voice)	Enables call fallback globally to RTP (nonsecure) mode.
srtp pass-thru (dial-peer)	Enables the transparent passthrough of unsupported crypto suites on an individual dial peer.
srtp system	Enables secure calls on a global level.

srtp-auth

Note Effective Cisco IOS XE Everest Releases 16.5.1b, **srtp-auth** command is deprecated. Although this command is still available in Cisco IOS XE Everest software, executing this command does not cause any configuration changes. Use **voice class srtp-crypto** command to configure SRTP connection using preferred crypto-suites. For more information, see voice class srtp-crypto command documentation.

To configure a Secure Real-time Transport Protocol (SRTP) connection on Cisco Unified Border Element (Cisco UBE) using the preferred crypto suite in the global level, use the **srtp-auth** command in the SIP configuration mode. To disable this configuration, use the **no** form of the command.

srtp-auth {**sha1-32** | **sha1-80**}
no srtp-auth

Syntax Description

sha1-32	Allows Secure calls with AES_CM_128_HMAC_SHA1_32 crypto suite.
sha1-80	Allow Secure calls with AES_CM_128_HMAC_SHA1_80 crypto suite.

Command Default

AES_CM_128_HMAC_SHA1_32 crypto suite is selected.

Command Modes

SIP configuration mode (conf-serv-sip)

Command History

Release	Modification
15.4(1)T	This command was introduced.
Cisco IOS XE Everest 16.5.1b	This command was deprecated.

Example

The following example shows how to configure an SRTP connection on Cisco UBE in the global level using the AES_CM_128_HMAC_SHA1_80 crypto suite:

```
Device> enable
Device# configure terminal
Device(config)# voice service voip
Device(conf-voi-serv)# sip
Device(conf-serv-sip)# srtp-auth sha1-80
Device(conf-serv-sip)# end
```

Related Commands

Command	Description
show sip-ua srtp	Displays Session Initiation Protocol (SIP) user-agent (UA) Secure Real-time Transport Protocol (SRTP) information.

Command	Description
voice-class sip srtp-auth	Configures a Secure Real-time Transport Protocol (SRTP) connection on Cisco Unified Border Element (CUBE) in the dial peer level using the preferred crypto suite.

srtp-crypto

To assign a previously configured crypto-suite selection preference list globally or to a voice class tenant, use the **srtp-crypto** command. To remove the crypto-suite selection preference and return to default preference list, use the **no** or **default** form of this command.

srtp-crypto *crypto-tag*
no srtp-crypto
default srtp-crypto

Syntax Description

crypto-tag	Unique number assigned to the voice class. The range is from 1 to 10000. This number maps to the tag created using the **voice class srtp-crypto** command available in global configuration mode.

Command Default

No crypto-suite preference assigned.

Command Modes

voice class tenant configuration (config-class)

voice service voice sip configuration (conf-serv-sip)

Command History

Release	Modification
Cisco IOS XE Everest 16.5.1b	This command was introduced.

Usage Guidelines

Note Ensure that srtp voice-class is created using the **voice class srtp-crypto** *crypto-tag* command before executing the **srtp-crypto** *crypto tag* command to apply the crypto-tag under global or tenant configuration mode.

You can assign only one crypto-tag. If you assign another crypto-tag, the last crypto-tag assigned replaces the previous crypto-tag.

Example

Example for assigning a crypto-suite preference to a voice class tenant:

```
Device> enable
Device# configure terminal
Device(config)# voice class tenant 100
Device(config-class)# srtp-crypto 102
```

Example for assigning a crypto-suite preference globally:

```
Device> enable
Device# configure terminal
Device(config)# voice service voice
Device(conf-voi-serv)# sip
Device(conf-serv-sip)# srtp-crypto 102
```

Related Commands

Command	Description
voice class sip srtp-crypto	Enters voice class configuration mode and assigns an identification tag for a srtp-crypto voice class.
crypto	Specifies the preference for the SRTP cipher-suite that will be offered by Cisco Unified Border Element (CUBE) in the SDP in offer and answer.
show sip-ua calls	Displays active user agent client (UAC) and user agent server (UAS) information on Session Initiation Protocol (SIP) calls.
show sip-ua srtp	Displays Session Initiation Protocol (SIP) user-agent (UA) Secure Real-time Transport Protocol (SRTP) information.

srtp negotiate

To enable the Cisco IOS Session Initiation Protocol (SIP) gateway to accept and send a Real-Time Transport Protocol (RTP) Audio/Video Profile (AVP) at the global configuration level, use the **srtp negotiate** command in voice service VoIP SIP configuration mode or voice class tenant configuration mode. To disable accepting and sending the RTP AVP, use the **no** form of this command.

srtp negotiate cisco system
no srtp negotiate system

Syntax Description

cisco	Allows an RTP to answer an Secure Real-time Transport Protocol (SRTP) offer.
system	Specifies that the negotiate method use the global sip-ua value. This keyword is available only for the tenant mode to allow it to fallback to the global configurations.

Command Default

Support for accepting and sending the RTP AVP at the global configuration level is disabled.

Command Modes

Voice service VoIP SIP configuration (conf-serv-sip)

Voice class tenant configuration (config-class)

Command History

Release	Modification
12.4(15)XY	This command was introduced.
12.4(20)T	This command was integrated into Cisco IOS Release 12.4(20)T.
12.4(22)T	Support was extended to the Cisco Unified Border Element.
15.0(1)M	This command was integrated into Cisco IOS Release 15.0(1)M.
15.6(2)T and IOS XE Denali 16.3.1	This command was modified to include the keyword: **system**. This command is now available under voice class tenants.
Cisco IOS XE Dublin 17.10.1a	Introduced support for YANG models.

Usage Guidelines

The **srtp fallback** command enables a SIP gateway to allow SRTP fallback using SIP 4*xx* message responses. With the **srtp negotiate** command, a SIP gateway can be configured to accept and send an RTP (nonsecure) profile in response to an SRTP profile.

Use the **srtp negotiate** command in voice service SIP configuration mode to enable SRTP negotiation globally on a SIP gateway to accept and send nonsecure RTP profiles in response to SRTP offers. To override the global setting and specify this behavior for an individual dial peer on a Cisco IOS SIP gateway, use the **voice-class sip srtp negotiate** command in dial peer voice configuration mode.

There are two scenarios for SRTP negotiation when the **srtp negotiate** command is enabled:

- On a SIP gateway with the **srtp fallback** command enabled, the gateway accepts RTP answers to SRTP offers.
- On a SIP gateway with the **srtp fallback** command disabled, the gateway allows incoming SRTP calls and responds with an RTP answer.

These behaviors are accomplished using the "X-cisco-srtp-fallback" extension in the supported header of initial SIP messages involved in establishment of the session.

Examples

The following example shows how to accept and send an SRTP AVP at the global configuration level:

```
Device> enable

Device# configure
 terminal
Device(config)# voice
 service
 voip

Device(conf-voi-serv)# sip
Device(conf-serv-sip)# srtp negotiate cisco
```

The following example shows SRTP negotiation being enabled globally on a SIP gateway:

```
Device(conf-voi-serv)# sip
Device(conf-serv-sip)# srtp negotiate cisco
```

The following example shows SRTP negotiation being enabled globally in the voice class tenant configuration mode:

```
Router(config-class)# srtp negotiate system
```

Related Commands

Command	Description
srtp (dial peer)	Specifies that an individual dial peer use SRTP to enable secure calls and, optionally, enables fallback to RTP (overriding global settings).
srtp (voice)	Specifies use of SRTP to enable secure calls and, optionally, enables fallback to RTP globally on a Cisco IOS SIP gateway.
voice class sip srtp negotiate	Enables the Cisco IOS SIP gateway to accept and send an RTP AVP at the dial-peer configuration level.

srv version

To generate Domain Name System Server (DNS SRV) queries with either the RFC 2052 or RFC 2782 format, use the **srv version** command in SIP UA configuration mode. To reset to the default, use the **no** form of this command.

srv version {**1** | **2**}
no srv version

Syntax Description

1	Specifies the domain-name prefix of format protocol.transport. (RFC 2052 style).
2	Specifies the domain-name prefix of format _protocol._transport. (RFC 2782 style).

Command Default

2 (RFC 2782 style)

Command Modes

SIP UA configurationn (config-sip-ua)

Command History

Release	Modification
12.2(2)XB	This command was introduced.
12.2(2)XB1	This command was implemented on the Cisco AS5850.
12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T. Support for the Cisco AS5850 was not included in this release.
12.2(11)T	This command was integrated into Cisco IOS Release 12.2(11)T. This command is supported on the Cisco AS5850 in this release.
Cisco IOS XE Release 2.5	This command was integrated into Cisco IOS XE Release 2.5.

Usage Guidelines

Session Initiation Protocol (SIP) on Cisco VoIP gateways uses DNS SRV queries to determine the IP address of the user endpoint. The query string has a prefix in the form of "protocol.transport." (RFC 2052) or "_protocol._transport." (RFC 2782). The selected string is then attached to the fully qualified domain name (FQDN) of the next hop SIP server.

By configuring the value of 1, this command provides compatibility with older equipment that supports only RFC 2052.

Examples

The following example sets up the **srv version**command in the RFC 2782 style (underscores surrounding the protocol):

```
Router(config)# sip-ua
Router(config-sip-ua)# srv version 2
```

Related Commands

Command	Description
show sip-ua status	Displays SIP status.



ss7 mtp2-variant through switchover method

- ss7 mtp2-variant, on page 1179
- ss7 mtp2-variant bellcore, on page 1184
- ss7 mtp2-variant itu, on page 1186
- ss7 mtp2-variant ntt, on page 1188
- ss7 mtp2-variant ttc, on page 1190
- ss7 mtp2-variant itu-white, on page 1192
- ss7 session, on page 1194
- ss7 session cumack_t, on page 1197
- ss7 session kp_t, on page 1199
- ss7 session m_cumack, on page 1201
- ss7 session m_outseq, on page 1203
- ss7 session m_rcvnum, on page 1205
- ss7 session m_retrans, on page 1207
- ss7 session retrans_t, on page 1209
- ss7 set, on page 1211
- ss7 set failover-timer, on page 1213
- station-id name, on page 1214
- station-id number, on page 1216
- stats, on page 1218
- stcapp, on page 1219
- stcapp call-control mode, on page 1221
- stcapp feature callback, on page 1223
- stcapp ccm-group, on page 1224
- stcapp feature access-code, on page 1225
- stcapp feature callback, on page 1227
- stcapp feature speed-dial, on page 1228
- stcapp register capability, on page 1230
- stcapp security mode, on page 1232
- stcapp security trustpoint, on page 1234
- stcapp supplementary-services, on page 1236
- stcapp timer, on page 1237
- stream-service profile, on page 1238
- stun, on page 1239

- stun flowdata agent-id, on page 1240
- stun flowdata catlife, on page 1241
- stun flowdata keepalive, on page 1242
- stun flowdata shared-secret, on page 1244
- stun usage firewall-traversal flowdata, on page 1246
- stun usage ice lite, on page 1247
- subaddress, on page 1248
- subcell-mux, on page 1249
- subscription asnl session history, on page 1250
- subscription maximum, on page 1251
- supervisory answer dualtone, on page 1252
- supervisory custom-cptone, on page 1254
- supervisory disconnect, on page 1256
- supervisory disconnect anytone, on page 1257
- supervisory disconnect dualtone, on page 1259
- supervisory disconnect dualtone voice-class, on page 1261
- supervisory disconnect lcfo, on page 1263
- supervisory dualtone-detect-params, on page 1264
- supervisory sit us, on page 1266
- supplementary-service h225-notify cid-update (dal peer), on page 1269
- supplementary-service h225-notify cid-update (voice-service), on page 1271
- supplementary-service h450.2 (dial peer), on page 1273
- supplementary-service h450.2 (voice-service), on page 1274
- supplementary-service h450.3 (dial peer), on page 1275
- supplementary-service h450.3 (voice-service), on page 1276
- supplementary-service h450.7, on page 1277
- supplementary-service h450.12 (dial peer), on page 1279
- supplementary-service h450.12 (voice-service), on page 1280
- supplementary-service media-renegotiate, on page 1282
- supplementary-service qsig call-forward, on page 1283
- supplementary-service sip, on page 1285
- supported language, on page 1288
- suppress, on page 1290
- survivability single-register, on page 1291
- suspend-resume (SIP), on page 1292
- switchback interval, on page 1293
- switchback method, on page 1294
- switchover method, on page 1296

ss7 mtp2-variant

To configure a Signaling System 7 (SS7) signaling link, use the **ss7 mtp2-variant** command in global configuration mode. To restore the designated default, use the **no** form of this command.

ss7 mtp2-variant [**bellcore** *channel* | **itu-white channel** | **ntt** *channel* | **ttc** *channel*] [*parameters*]
no ss7 mtp2-variant

Syntax Description

bellcore	Configures the router for Telcordia Technologies (formerly Bellcore) standards.
channel	Message Transfer Part Layer 2 (MTP2) serial channel number. Range is from 0 to 3.
itu white	Configures the SS7 channel with the ITU-white protocol variant.
ntt	Configures the router for NTT (Japan) standards. **Note** This keyword is not available with the PCR feature.
ttc	Configures the router for Japanese Telecommunications Technology Committee (TTC) standards. **Note** This keyword is not available with the PCR feature.
parameters	(Optional) Configures a particular standard. See the tables in the "Usage Guidelines" section for accepted parameters.

Command Default

bellcore

Command Modes

Global configuration (config)

Command History

Release	Modification
12.0(7)XR	This command was introduced.
12.1(1)T	This command was integrated into Cisco IOS Release 12.1(1)T.
12.3(2)T	This command was modified to include all possible variants: **bellcore**, **itu white**, **ntt**, **ttc**.

Usage Guidelines

The MTP2 variant has timers and parameters that can be configured using the values listed in the following tables. To restore the designated default, use the **no** or the **default** form of the command (see the "Examples" section below).

Note When the **bellcore** or **itu white** variant is selected, this command enters a new configuration mode for setting MTP2 parameters: ITU configuration mode. See the **error correction**command reference for information about setting MTP2 parameters from this mode.

Table 226: Bellcore (Telcordia Technologies) Parameters and Values

Parameter	Description	Default	Range
T1	Aligned/ready timer duration (milliseconds)	13000	1000 to 65535
T2	Not aligned timer (milliseconds)	11500	1000 to 65535
T3	Aligned timer (milliseconds)	11500	1000 to 65535
T4 Emergency Proving	Emergency proving timer (milliseconds)	1600	1000 to 65535
T4 Normal Proving	Normal proving period (milliseconds)	2300	1000 to 65535
T5	Sending status indication busy (SIB) timer (milliseconds)	100	80 to 65535
T6	Remote congestion timer (milliseconds)	6000	1000 to 65535
T7	Excessive delay timer (milliseconds)	1000	500 to 65535
lssu len	1- or 2-byte link status signal unit (LSSU) format	1	1 to 2
unacked MSUs	Maximum number of message signal units (MSUs) awaiting acknowledgment (ACK)	127	16 to 127
proving attempts	Maximum number of attempts to prove alignment	5	3 to 8
SUERM threshold	Signal Unit Error Rate Monitor (SUERM) error-rate threshold	64	32 to 128
SUERM number octets	SUERM octet-counting mode	16	8 to 32
SUERM number signal units	Signal units (good or bad) needed to decrement Error Rate Monitor (ERM)	256	128 to 512
Tie AERM Emergency	Alignment Error Rate Monitor (AERM) emergency error-rate threshold	1	1 to 8
Tie AERM Normal	AERM normal error-rate threshold	4	1 to 8

Table 227: ITU-white Parameters and Values

Parameter	Description	Default	Range
T1	Aligned/ready timer duration (milliseconds)	40000	1000 to 65535
T2	Not aligned timer (milliseconds)	5000	1000 to 65535
T3	Aligned timer (milliseconds)	1000	1000 to 65535
T4 Emergency Proving	Emergency proving timer (milliseconds)	500	1000 to 65535
T4 Normal Proving	Normal proving timer (milliseconds)	8200	1000 to 65535
T5	Sending SIB timer (milliseconds)	100	80 to 65535

Parameter	Description	Default	Range
T6	Remote congestion timer (milliseconds)	6000	1000 to 65535
T7	Excessive delay timer (milliseconds)	1000	1000 to 65535
lssu len	1- or 2-byte link status signal unit (LSSU) format	1	1 to 2
msu len	message signal unit (MSU) length	1	1 to 2
unacked MSUs	Maximum number of MSUs awaiting acknowledgment (ACK)	127	16 to 127
proving attempts	Maximum number of attempts to prove alignment	5	3 to 8
SUERM threshold	Signal Unit Error Rate Monitor (SUERM) error-rate threshold	64	32 to 128
SUERM number octets	SUERM octet counting mode	16	8 to 32
SUERM - number - signal - units	Signal units (good or bad) needed to decrement Error Rate Monitor (ERM)	256	128 to 512
Tie AERM Emergency	Alignment Error Rate Monitor (AERM) emergency error-rate threshold	1	1 to 8
Tin AERM Normal	AERM normal error-rate threshold	4	1 to 8

Table 228: NTT Parameters and Values

Parameter	Description	Default	Range
T1	Aligned/ready timer duration (milliseconds)	15000	1000 to 65535
T2	Not aligned timer (milliseconds)	5000	1000 to 65535
T3	Aligned timer (milliseconds)	3000	1000 to 65535
T4 Emergency Proving	Emergency proving timer (milliseconds)	3000	1000 to 65535
T5	Sending SIB timer (milliseconds)	200	80 to 65535
T6	Remote congestion timer (milliseconds)	2000	1000 to 65535
T7	Excessive delay timer (milliseconds)	3000	1000 to 65535
TA	SIE interval timer (milliseconds)	20	10 to 500
TF	Fill-in Signal Unit (FISU) interval timer (milliseconds)	20	10 to 500
TO	SIO interval timer (milliseconds)	20	10 to 500
TS	SIOS interval timer (milliseconds)	20	10 to 500

Parameter	Description	Default	Range
unacked MSUs	Maximum number of message signal units (MSUs) awaiting acknowledgment (ACK)	40	16 to 40
proving attempts	Maximum number of attempts to prove alignment	5	3 to 8
SUERM threshold	Signal Unit Error Rate Monitor (SUERM) e error-rate threshold	64	32 to 128
SUE RM - number - octets	SUERM octet counting mode	16	8 to 32
SUERM - number - signal - units	Signal Unit Error Rate Monitor (SUERM) units (good or bad) needed to decrement Error Rate Monitor (ERM)	256	128 to 512
Tie - AERM - Emergency	Alignment Error Rate Monitor (AERM) emergency error-rate threshold	1	1 to 8

Table 229: TTC Parameters and Values

Parameter	Description	Default	Range
T1	Aligned/ready timer duration (milliseconds)	15000	1000 to 65535
T2	Not aligned timer (milliseconds)	5000	1000 to 65535
T3	Aligned timer (milliseconds)	3000	1000 to 65535
T4 Emergency Proving	Emergency proving timer (milliseconds)	3000	1000 to 65535
T5	Sending SIB timer (milliseconds)	200	80 to 65535
T6	Remote congestion timer (milliseconds)	2000	1000 to 65535
T7	Excessive delay timer (milliseconds)	3000	1000 to 65535
TA	SIE interval timer (milliseconds)	20	10 to 500
TF	FISU interval timer (milliseconds)	20	10 to 500
TO	SIO interval timer (milliseconds)	20	10 to 500
TS	SIOS interval timer (milliseconds)	20	10 to 500
unacked MSUs	Maximum number of message signal units (MSUs) awaiting acknowledgment (ACK)	40	16 to 40
proving attempts	Maximum number of attempts to prove alignment	5	3 to 8
SUERM threshold	Signal Unit Error Rate Monitor (SUERM) error - rate threshold	64	32 to 128
SUERM number octets	SUERM octet counting mode	16	8 to 32

Parameter	Description	Default	Range
SUERM number signal units	Signal units (good or bad) needed to decrement ERM	256	128 to 512
Tie AERM Emergency	AERM emergency error-rate threshold	1	1 to 8

Examples

The following example configures an SS7 channel (link) for Preventive Cyclic Retransmission (PCR) with forced retransmission initiated. In this example, SS7 channel 0 is configured with the ITU-white protocol variant using the PCR error correction method.

```
Router# configure terminal
Router(config)# ss7 mtp2-variant itu-white 0

Router(config-ITU)# error-correction pcr forced-retransmission enabled N2 1000
Router(config-ITU)# end
```

The following example disables error-correction:

```
Router(config-ITU)# no error-correction
```

Related Commands

Command	Description
error correction	Sets the error correction method for the SS7 signaling link when the SS7 MTP2 variant is Bellcore or ITU-white.
show ss7 mtp2 ccb	Displays SS7 MTP2 CCB information.
show ss7 mtp2 state	Displays internal SS7 MTP2 state machine information.

ss7 mtp2-variant bellcore

To configure the router for Telcordia Technologies (formerly Bellcore) standards, use the **ss7 mtp2-variant bellcore** command in global configuration mode.

ss7 mtp2-variant bellcore [*channel*] [*parameters*]

Syntax Description

channel	(Optional) Channel. Range is from 0 to 3.
parameters	(Optional) Particular Bellcore standard. See the table below for descriptions, defaults, and ranges.

Command Default

Bellcore is the default variant if no other is configured. See the table below for default parameters.

Command Modes

Global configuration(config)

Command History

Release	Modification
12.0(7)XR	This command was introduced.
12.1(1)T	This command was integrated into Cisco IOS Release 12.1(1)T.

Usage Guidelines

This MTP2 variant has timers and parameters that can be configured using the values listed in the table below. To restore the designated default, use the **no** or the **default** form of the command (see example below).

Note Timer durations are converted to 10-millisecond units. For example, a T1 value of 1005 is converted to 100, which results in an actual timeout duration of 1000 ms. This is true for all timers and all variants.

Table 230: Bellcore (Telcordia Technologies) Parameters and Values

Parameter	Description	Default	Range
T1	Aligned/ready timer duration (milliseconds)	13000	1000 to 65535
T2	Not aligned timer (milliseconds)	11500	1000 to 65535
T3	Aligned timer (milliseconds)	11500	1000 to 65535
T4 -Emergency-Proving	Emergency proving timer (milliseconds)	600	1000 to 65535
T4 -Normal-Proving	Normal proving period (milliseconds)	2300	1000 to 65535
T5	Sending SIB timer (milliseconds)	100	80 to 65535
T6	Remote congestion timer (milliseconds)	6000	1000 to 65535
T7	Excessive delay timer (milliseconds)	1000	500 to 65535

Parameter	Description	Default	Range
lssu -len	1- or 2-byte LSSU format	1	1 to 2
unacked -MSUs	Maximum number of MSUs waiting ACK	127	16 to 127
proving -attempts	Maximum number of attempts to prove alignment	5	3 to 8
SUERM -threshold	SUERM error-rate threshold	64	32 to 128
SUERM -number-octets	SUERM octet-counting mode	16	8 to 32
SUERM -number-signal units	Signal units (good or bad) needed to dec ERM	256	128 to 512
Tie -AERM-Emergency	AERM emergency error-rate threshold	1	1 to 8
Tie -AERM-Normal	AERM normal error-rate threshold	4	1 to 8

Examples

The following example sets the aligned/ready timer duration on channel 0 to 30,000 ms:

```
ss7 mtp2-variant bellcore 0 T1 30000
```

The following example restores the aligned/ready timer default value of 13,000 ms:

```
ss7 mtp2-variant bellcore 0 no T1
```

Related Commands

Command	Description
ss7 mtp2 -variant itu	Specifies the MTP2-variant as ITU.
ss7 mtp2 -variant ntt	Specifies the MTP2-variant as NTT.
ss7 mtp2 -variant ttc	Specifies the MTP2-variant as TTC.

ss7 mtp2-variant itu

To configure the router for ITU (International Telecom United) standards, use the **ss7 mtp2-variant itu** command in global configuration mode.

ss7 mtp-variant itu [*channel*] [*parameters*]

Syntax Description

channel	Channel. Range is from 0 to 3.
parameters	(Optional) Particular Bellcore standard. See the table below for descriptions, defaults, and ranges.

Command Default

Bellcore is the default variant if no other is configured. See the table below for ITU default parameters.

Command Modes

Global configuration

Command History

Release	Modification
12.0(7)XR	This command was introduced.
12.1(1)T	This command was integrated into Cisco IOS Release 12.1(1)T.

Usage Guidelines

The ITU MTP2 variant has timers and parameters that can be configured using the values listed in the table below. To restore the designated default, use the **no** or the **default** form of the command (see the example below).

Table 231: ITU (White) Parameters and Values

Parameter	Description	Default	Range
T1	Aligned/ready timer duration (milliseconds)	40000	1000 to 65535
T2	Not aligned timer (milliseconds)	5000	1000 to 65535
T3	Aligned timer (milliseconds)	1000	1000 to 65535
T4 -Emergency-Proving	Emergency proving timer (milliseconds)	500	1000 to 65535
T4 -Normal-Proving	Normal proving timer (milliseconds)	8200	1000 to 65535
T5	Sending SIB timer (milliseconds)	100	80 to 65535
T6	Remote congestion timer (milliseconds)	6000	1000 to 65535
T7	Excessive delay timer (milliseconds)	1000	1000 to 65535
lssu -len	1- or 2-byte LSSU format	1	1 to 2
msu -len			

Parameter	Description	Default	Range
unacked -MSUs	Maximum number of MSUs waiting ACK	127	16 to 127
proving -attempts	Maximum number of attempts to prove alignment	5	3 to 8
SUERM -threshold	SUERM error rate threshold	64	32 to 128
SUERM -number-octets	SUERM octet counting mode	16	8 to 32
SUERM -number-signal units	Signal units (good or bad) needed to dec ERM	256	128 to 512
Tie -AERM-Emergency	AERM emergency error-rate threshold	1	1 to 8
Tin -AERM-Normal	AERM normal error-rate threshold	4	1 to 8

Examples

The following example sets the emergency proving period on channel 1 to 10,000 ms:

```
ss7 mtp2-variant itu 1
 t4-Emergency-Proving 10000
```

The following example restores the emergency proving period default value of 5,000 ms:

```
ss7 mtp2-variant itu 1
 default t4-Emergency-Proving
```

Related Commands

Command	Description
ss7 mtp2-variant bellcore	Specifies the MTP2-variant as Bellcore.
ss7 mtp2-variant ntt	Specifies the MTP2-variant as NTT.
ss7 mtp2-variant ttc	Specifies the MTP2-variant as TTC.

ss7 mtp2-variant ntt

To configure the router for NTT (Japan) standards, use the **ss7 mtp2-variant ntt** command in global configuration mode.

ss7 mtp-variant ntt [*channel*] [*parameters*]

Syntax Description

channel	Channel. Range is from 0 to 3.
parameters	(Optional) Particular Telcordia Technologies (formerly Bellcore) standard. See the table below for descriptions, defaults, and ranges.

Command Default

Bellcore is the default variant if no other is configured. See the table below for NTT default parameters.

Command Modes

Global configuration

Command History

Release	Modification
12.0(7)XR	This command was introduced.
12.1(1)T	This command was integrated into Cisco IOS Release 12.1(1)T.

Usage Guidelines

The NTT MTP2 variant has timers and parameters that can be configured using the values listed in the table below. To restore the designated default, use the **no** or the **default** form of the command (see the example below).

Table 232: NTT Parameters and Values

Parameter	Description	Default	Range
T1	Aligned/ready timer duration (milliseconds)	15000	1000 to 65535
T2	Not aligned timer (milliseconds)	5000	1000 to 65535
T3	Aligned timer (milliseconds)	3000	1000 to 65535
T4 -Emergency-Proving	Emergency proving timer (milliseconds)	3000	1000 to 65535
T5	Sending SIB timer (milliseconds)	200	80 to 65535
T6	Remote congestion timer (milliseconds)	2000	1000 to 65535
T7	Excessive delay timer (milliseconds)	3000	1000 to 65535
TA	SIE interval timer (milliseconds)	20	10 to 500
TF	FISU interval timer (milliseconds)	20	10 to 500
TO	SIO interval timer (milliseconds)	20	10 to 500

Parameter	Description	Default	Range
TS	SIOS interval timer (milliseconds)	20	10 to 500
unacked -MSUs	Maximum number of MSUs waiting ACK	40	16 to 40
proving -attempts	Maximum number of attempts to prove alignment	5	3 to 8
SUERM -threshold	SUERM error rate threshold	64	32 to 128
SUERM -number-octets	SUERM octet counting mode	16	8 to 32
SUERM -number-signal units	Signal units (good or bad) needed to dec ERM	256	128 to 512
Tie -AERM-Emergency	AERM emergency error-rate threshold	1	1 to 8

Examples

The following example sets the SUERM error rate threshold on channel 2 to 100:

```
ss7 mtp2-variant ntt 2
 SUERM-threshold 100
```

The following example restores the SUERM error rate threshold default value of 64:

```
ss7 mtp2-variant ntt 2
 no SUERM-threshold
```

Related Commands

Command	Description
ss7 mtp2-variant bellcore	Specifies the MTP2-variant as Bellcore.
ss7 mtp2-variant itu	Specifies the MTP2-variant as ITU.
ss7 mtp2-variant ttc	Specifies the MTP2-variant as TTC.

ss7 mtp2-variant ttc

To configure the router for TTC (Japan Telecom) standards, use the **ss7 mtp2-variant ttc** command in global configuration mode.

ss7 mtp-variant ttc [*channel*] [*parameters*]

Syntax Description

channel	Channel. Range is from 0 to 3.
parameters	(Optional) Particular Telcordia Technologies (formerly Bellcore) standard. See the table below for descriptions, defaults, and ranges.

Command Default

Bellcore is the default variant if no other is configured. See the table below for TTC default parameters.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.0(7)XR	This command was introduced.
12.1(1)T	This command was integrated into Cisco IOS Release 12.1(1)T.

Usage Guidelines

The TTC MTP2 variant has timers and parameters that can be configured using the values listed in the table below. To restore the designated default, use the **no** or the **default** form of the command (see the example below).

Table 233: TTC Parameters and Values

Parameter	Description	Default	Range
T1	Aligned/ready timer duration (milliseconds)	15000	1000 to 65535
T2	Not aligned timer (milliseconds)	5000	1000 to 65535
T3	Aligned timer (milliseconds)	3000	1000 to 65535
T4 -Emergency-Proving	Emergency proving timer (milliseconds)	3000	1000 to 65535
T5	Sending SIB timer (milliseconds)	200	80 to 65535
T6	Remote congestion timer (milliseconds)	2000	1000 to 65535
T7	Excessive delay timer (milliseconds)	3000	1000 to 65535
TA	SIE interval timer (milliseconds)	20	10 to 500
TF	FISU interval timer (milliseconds)	20	10 to 500
TO	SIO interval timer (milliseconds)	20	10 to 500

Parameter	Description	Default	Range
TS	SIOS interval timer (milliseconds)	20	10 to 500
unacked -MSUs	Maximum number of MSUs waiting ACK	40	16 to 40
proving -attempts	Maximum number of attempts to prove alignment	5	3 to 8
SUERM -threshold	SUERM error rate threshold	64	32 to 128
SUERM -number-octets	SUERM octet counting mode	16	8 to 32
SUERM -number-signal-units	Signal units (good or bad) needed to dec ERM	256	128 to 512
Tie -AERM-Emergency	AERM emergency error-rate threshold	1	1 to 8

Examples

The following example sets the maximum number of proving attempts for channel 3 to 3:

```
ss7 mtp2-variant ttc 3
 proving-attempts 3
```

The following example restores the maximum number of proving attempts to the default value:

```
ss7 mtp2-variant ttc 3
 default proving-attempts
```

Related Commands

Command	Description
ss7 mtp2 -variant bellcore	Specifies the MTP2-variant as Bellcore.
ss7 mtp2 -variant itu	Specifies the MTP2-variant as ITU.
ss7 mtp2 -variant ntt	Specifies the MTP2-variant as NTT.

ss7 mtp2-variant itu-white

To configure the router for International Telecommunications Union (ITU) standards, use the **ss7 mtp2-variant itu-white** command in global configuration mode.

ss7 mtp2-variant itu-white [*channel*] [*parameters*]

Syntax Description

channel	(Optional) Message Transfer Part 2 (MTP2) serial channel number. The range is from 0 to 3.
parameters	(Optional) Particular Bellcore standard. See the table below for descriptions, defaults, and ranges.

Command Default

Bellcore is the default variant if no other is configured. See the table below for ITU default parameters.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.0(7)XR	This command was introduced.
12.1(1)T	This command was integrated into Cisco IOS Release 12.1(1)T.

Usage Guidelines

The ITU MTP2 variant has timers and parameters that can be configured using the values listed in the table below. To restore the designated default, use the **no** or the **default** form of the command.

Table 234: ITU (White) Parameters and Values

Parameter	Description	Default	Range
T1	Aligned/ready timer duration (milliseconds [ms])	40000	1000 to 65535
T2	Not aligned timer (ms)	5000	1000 to 65535
T3	Aligned timer (ms)	1000	1000 to 65535
T4-Emergency-Proving	Emergency proving timer (ms)	500	1000 to 65535
T4-Normal-Proving	Normal proving timer (ms)	8200	1000 to 65535
T5	Sending SIB timer (ms)	100	80 to 65535
T6	Remote congestion timer (ms)	6000	1000 to 65535
T7	Excessive delay timer (ms)	1000	1000 to 65535
lssu-len	1- or 2-byte Links Status Signal Unit (LSSU) format	1	1 to 2
msu-len	--	--	--

Parameter	Description	Default	Range
unacked-MSUs	Maximum number of Message Signal Units (MSUs) waiting acknowledgement	127	16 to 127
proving-attempts	Maximum number of attempts to prove alignment	5	3 to 8
SUERM-threshold	Signal unit error monitor (SUERM) error rate threshold	64	32 to 128
SUERM-number-octets	SUERM octet counting mode	16	8 to 32
SUERM-number-signal- units	Signal units (good or bad) needed to dec Embedded Resource Manager (ERM)	256	128 to 512
Tie-AERM-Emergency	Alignment Unit Error Rate Monitor (AERM) emergency error-rate threshold	1	1 to 8
Tin-AERM-Normal	AERM normal error-rate threshold	4	1 to 8

Examples

The following example shows how to set the emergency proving period on channel 1 to 10,000 ms:

```
Router(config)# ss7 mtp2-variant itu-white 1
Router(config-ITU)# t4-Emergency-Proving 10000
```

The following example shows how to restore the emergency proving period default value of 5000 ms:

```
Router(config)# ss7 mtp2-variant itu-white 1
Router(config-ITU)# default t4-Emergency-Proving 5000
```

Related Commands

Command	Description
ss7 mtp2-variant bellcore	Specifies the MTP2 variant as Bellcore.
ss7 mtp2-variant ntt	Specifies the MTP2 variant as NTT.
ss7 mtp2-variant ttc	Specifies the MTP2 variant as TTC.

ss7 session

To create a Reliable User Datagram Protocol (RUDP) session and explicitly add an RUDP session to a Signaling System 7 (SS7) session set, use the **ss7 session** command in global configuration mode. To delete the session, use the **no** form of this command.

ss7 session *session-id* **address** *destination-address destinaion-port local-address local-port* [**session-set** *session-number*]
no ss7 session *session-id*

Syntax Description

session -id	SS7 session number. Valid values are 0 and 1. You must enter a hyphen with no space following it after the **session** keyword.
address *destination -address*	Specifies the SS7 session IP address.
destination -address	The local IP address of the router in four-part dotted-decimal format. The local IP address for both sessions, 0 and 1, must be the same.
destination -port	The number of the local UDP port on which the router expects to receive messages from the media gateway controller (MGC) . Specify any UDP port that is not used by another protocol as defined in RFC 1700 and that is not otherwise used in your network. The local UDP port must be different for session 0 and session 1. Valid port ranges are from 1024 to 9999.
local -address	The remote IP address of the MGC in four-part dotted-decimal format.
local -port	The number of the remote UDP port on which the MGC is configured to listen. This UDP port cannot be used by another protocol as defined in RFC 1700 and cannot be otherwise used in the network. Valid port ranges are from 1024 to 9999.
session -setsession - number	(Optional) Assigns an SS7 session to an SS7 session set.

Command Default

No session is configured.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.0(7)XR	This command was introduced.
12.1(1)T	This command was integrated into Cisco IOS Release 12.1(1)T.
12.2(15)T	The **session-set** keyword and thesession - number argument were added.

Usage Guidelines

For the Cisco 2600-based SLT, you can configure a maximum of four sessions, two for each Cisco SLT. In a redundant VSC configuration, session 0 and session 2 are configured to one VSC, and session 1 and session 3 are configured to the other. Session 0/1 and session 2/3 run to the Cisco SLT.

The VSC must be configured to send messages to the local port, and it must be configured to listen on the remote port. You must also reload the router whenever you remove a session or change the parameters of a session.

This command replaces the **ss7 session-0 address** and **ss7 session-1 address** commands, which contain hard-coded session numbers. The new command is used for the new dual Ethernet capability.

The new CLI supports both single and dual Ethernet configuration by being backward compatible with the previous **session-0** and **session-1** commands so that you can configure a single Ethernet instead of two, if needed.

For the Cisco AS5350 and Cisco AS5400-based SLT, you can configure a maximum of two sessions, one for each signaling link. In a redundant MGC configuration, session 0 is configured to one MGC and session 1 is configured to the other.

The MGC must be configured to send messages to the local port, and the MGC must be configured to listen on the remote port.

You must reload the router whenever you remove a session or change the parameters of a session.

By default, each RUDP session must belong to SS7 session set 0. This allows backward compatibility with existing SS7 configurations.

If the **session-set** keyword is omitted, the session is added to the default SS7 session set 0. This allows backward compatibility with older configurations. Entering the no form of the command is still sufficient to remove the session ID for that RUDP session.

If you want to change the SS7 session set to which a session belongs, you have to remove the entire session first. This is intended to preserve connection and recovery logic.

Examples

The following example sets up two sessions on a Cisco 2611 and creates session set 2:

```
ss7 session-0 address 172.16.1.0 7000 172.16.0.0 7000 session-set 2
ss7 session-1 address 172.17.1.0 7002 172.16.0.0 7001 session-set 2
```



Note The example above shows how the local IP addresses in session-0 and session-1 must be the same.

Related Commands

Command	Description
ss7 session cumack_t	Sets the cumulative acknowledgment timer.
ss7 session k_pt	Sets the null segment (keepalive) timer.
ss7 session m_cumack	Sets the maximum number of segments that can be received before the RUDP sends an acknowledgment.
ss7 session m_outseq	Sets the maximum number of out-of-sequence segments that can be received before the RUDP sends an extended acknowledgment.

Command	Description
ss7 session m_rcvnum	Sets the maximum number of segments that the remote end can send before receiving an acknowledgment.
ss7 session m_retrans	Sets the maximum number of times that the RUDP attempts to resend a segment before declaring the connection invalid.
ss7 session retrans_t	Sets the retransmission timer.

ss7 session cumack_t

To set the Reliable User Datagram Protocol (RUDP) cumulative acknowledgment timer for a specific SS7 signaling link session, use the **ss7 session cumack_t**command in global configuration mode. To reset to the default, use the **no** form of this command.

ss7 session *session-number* **cumack_t** *milliseconds*
no ss7 session *session-number* **cumack_t**

Syntax Description

session -number	SS7 session number. Valid values are 0 and 1. You must enter the hyphen, with no space following it, after the **session** keyword.
milliseconds	Interval, in milliseconds, that the RUDP waits before it sends an acknowledgment after receiving a segment. Range is from 100 to 65535. The value should be less than the value configured for the retransmission timer by using the ss7 session-*session number* **retrans_t**command.

Command Default

300 ms

Command Modes

Global configuration (config)

Command History

Release	Modification
12.0(7)XR	This command was introduced.
12.1(1)T	This command was integrated into Cisco IOS Release 12.1(1)T.

Usage Guidelines

The cumulative acknowledgment timer determines when the receiver sends an acknowledgment. If the timer is not already running, it is initialized when a valid data, null, or reset segment is received. When the cumulative acknowledgment timer expires, the last in-sequence segment is acknowledged. The RUDP typically tries to "piggyback" acknowledgments on data segments being sent. However, if no data segment is sent in this period of time, it sends a standalone acknowledgment.



Caution Use the default setting. Do not change session timers unless instructed to do so by Cisco technical support. Changing timers may result in service interruption or outage.

Examples

The following example sets up two sessions and sets the cumulative acknowledgment timer to 320 ms for each one:

```
ss7 session-0 address 255.255.255.251 7000 255.255.255.254 7000
ss7 session-0 cumack_t 320
ss7 session-1 address 255.255.255.253 7002 255.255.255.254 7001
ss7 session-1 cumack_t 320
```

Related Commands

Command	Description
show ss7	Displays the SS7 configuration.
ss7 session k_pt	Sets the null segment (keepalive) timer.
ss7 session m_cumack	Sets the maximum number of segments that can be received before the RUDP sends an acknowledgment.
ss7 session m_outseq	Sets the maximum number of out-of-sequence segments that can be received before the RUDP sends an extended acknowledgment.
ss7 session m_rcvnum	Sets the maximum number of segments that the remote end can send before receiving an acknowledgment.
ss7 session m_retrans	Sets the maximum number of times that the RUDP attempts to resend a segment before declaring the connection invalid.
ss7 session retrans_t	Sets the retransmission timer.

ss7 session kp_t

To set the null segment (keepalive) timer for a specific SS7 signaling link session, use the **ss7 session kp_t**command in global configuration mode. To reset to the default, use the **no** form of this command.

ss7 session-session *number* **kp_t milliseconds**
no ss7 session-session *number* **kp_t milliseconds**

Syntax Description

session -number	SS7 session number. Valid values are 0 and 1. You must enter the hyphen, with no space following it, after the **session** keyword.
milliseconds	Interval, in milliseconds, that the Reliable User Datagram Protocol (RUDP) waits before sending a keepalive to verify that the connection is still active. Valid values are 0 and from100 to 65535. Default is 2000.

Command Default

2000 ms

Command Modes

Global configuration (config)

Command History

Release	Modification
12.0(7)XR	This command was introduced.
12.1(1)T	This command was integrated into Cisco IOS Release 12.1(1)T.

Usage Guidelines

Caution Use the default setting. Do not change session timers unless instructed to do so by Cisco technical support. Changing timers may result in service interruption or outage.

The null segment timer determines when a null segment (keepalive) is sent by the client Cisco 2600 series router. On the client, the timer starts when the connection is established and is reset each time a data segment is sent. If the null segment timer expires, the client sends a keepalive to the server to verify that the connection is still functional. On the server, the timer restarts each time a data or null segment is received from the client.

The value of the server's null segment timer is twice the value configured for the client. If no segments are received by the server in this period of time, the connection is no longer valid.

To disable keepalive, set this parameter to 0.

Examples

The following example sets up two sessions and sets a keepalive of 1,800 ms for each one:

```
ss7 session-0 address 255.255.255.251 7000 255.255.255.254 7000
ss7 session-0 kp_t 1800
ss7 session-1 address 255.255.255.253 7002 255.255.255.254 7001
ss7 session-1 kp_t 1800
```

Related Commands

Command	Description
show ss7	Displays the SS7 configuration.
ss7 session cumack_t	Sets the cumulative acknowledgment timer.
ss7 session m_cumack	Sets the maximum number of segments that can be received before the RUDP sends an acknowledgment.
ss7 session m_outseq	Sets the maximum number of out-of-sequence segments that can be received before the RUDP sends an extended acknowledgment.
ss7 session m_rcvnum	Sets the maximum number of segments that the remote end can send before receiving an acknowledgment.
ss7 session m_retrans	Sets the maximum number of times that the RUDP attempts to resend a segment before declaring the connection invalid.
ss7 session retrans_t	Sets the retransmission timer.

ss7 session m_cumack

To set the maximum number of segments that can be received before the Reliable User Datagram Protocol (RUDP) sends an acknowledgment in a specific SS7 signaling link session, use the **ss7 session m_cumack**command in global configuration mode. To reset to the default, use the **no** form of this command.

ss7 session-session *number* **m_cumack** *segments*
no ss7 session-session *number* **m_cumack** *segments*

Syntax Description

session -number	SS7 session number. Valid values are 0 and 1. You must enter the hyphen, with no space following it, after the **session** keyword.
segments	Maximum number of segments that can be received before the Reliable User Datagram Protocol (RUDP) sends an acknowledgment. Range is from 0 to 255. Default is 3.

Command Default

3 segments

Command Modes

Global configuration (config)

Command History

Release	Modification
12.0(7)XR	This command was introduced.
12.1(1)T	This command was integrated into Cisco IOS Release 12.1(1)T.

Usage Guidelines

Caution Use the default setting. Do not change session timers unless instructed to do so by Cisco technical support. Changing timers may result in service interruption or outage.

The cumulative acknowledgment counter records the number of unacknowledged, in-sequence data, null, or reset segments received without a data, null, or reset segment being sent to the transmitter. If this counter reaches the configured maximum, the receiver sends a standalone acknowledgment (a standalone acknowledgment is a segment that contains only acknowledgment information). The standalone acknowledgment contains the sequence number of the last data, null, or reset segment received.

If you set this parameter to 0, an acknowledgment is sent immediately after a data, null, or reset segment is received.

Examples

The following example sets up two sessions and in each session sets a maximum of two segments for receipt before acknowledgment:

```
ss7 session-0 address 255.255.255.251 7000 255.255.255.254 7001
ss7 session-0 m_cumack 2
ss7 session-1 address 255.255.255.253 7002 255.255.255.254 7000
ss7 session-1 m_cumack 2
```

Related Commands

Command	Description
show ss7	Displays the SS7 configuration.
ss7 session cumack_t	Sets the cumulative acknowledgment timer.
ss7 session k_pt	Sets the null segment (keepalive) timer.
ss7 session m_outseq	Sets the maximum number of out-of-sequence segments that can be received before the RUDP sends an extended acknowledgment.
ss7 session m_rcvnum	Sets the maximum number of segments that the remote end can send before receiving an acknowledgment.
ss7 session m_retrans	Sets the maximum number of times that the RUDP attempts to resend a segment before declaring the connection invalid.
ss7 session retrans_t	Sets the retransmission timer.

ss7 session m_outseq

To set the maximum number of out-of-sequence segments that can be received before the Reliable User Datagram Protocol (RUDP) sends an extended acknowledgment in a specific SS7 signaling link session, use the **ss7 session m_outseq**command in global configuration mode. To reset to the default, use the **no** form of this command.

ss7 session-session *number* **m_outseq** *segments*
no ss7 session-session *number* **m_outseq**

Syntax Description

session -number	SS7 session number. Valid values are 0 and 1. You must enter the hyphen, with no space following it, after the **session** keyword.
segments	Maximum number of out-of-sequence segments that can be received before the RUDP sends an extended acknowledgment. If the specified number of segments are received out of sequence, an Extended Acknowledgment segment is sent to inform the sender which segments are missing. Range is from 0 to 255. Default is 3.

Command Default

3 segments

Command Modes

Global configuration (config)

Command History

Release	Modification
12.0(7)XR	This command was introduced.
12.1(1)T	This command was integrated into Cisco IOS Release 12.1(1)T.

Usage Guidelines



Caution Use the default setting. Do not change session timers unless instructed to do so by Cisco technical support. Changing timers may result in service interruption or outage.

The out-of-sequence acknowledgment counter records the number of data segments that have arrived out of sequence. If this counter reaches the configured maximum, the receiver sends an extended acknowledgment segment that contains the sequence numbers of the out-of-sequence data, null, and reset segments received. When the transmitter receives the extended acknowledgment segment, it retransmits the missing data segments.

If you set this parameter to 0, an acknowledgment is sent immediately after an out-of-sequence segment is received.

Examples

The following example sets up two sessions and sets a maximum number of four out-of-sequence segments for each session:

```
ss7 session-0 address 255.255.255.251 7000 255.255.255.254 7001
ss7 session-0 m_outseq 4
```

```
ss7 session-1 address 255.255.255.253 7002 255.255.255.254 7000
ss7 session-1 m_outseq 4
```

Related Commands

Command	Description
show ss7	Displays the SS7 configuration.
ss7 session cumack_t	Sets the cumulative acknowledgment timer.
ss7 session k_pt	Sets the null segment (keepalive) timer.
ss7 session m_cumack	Sets the maximum number of segments that can be received before the RUDP sends an acknowledgment.
ss7 session m_rcvnum	Sets the maximum number of segments that the remote end can send before receiving an acknowledgment.
ss7 session m_retrans	Sets the maximum number of times that the RUDP attempts to resend a segment before declaring the connection invalid.
ss7 session retrans_t	Sets the retransmission timer.

ss7 session m_rcvnum

To set the maximum number of segments that the remote end can send before receiving an acknowledgment in a specific SS7 signaling link session, use the **ss7 session m_rcvnum**command in global configuration mode. To reset to the default, use the **no** form of this command.

ss7 session-session *number* **m_rcvnum** *segments*
no ss7 session-session *number* **m_rcvnum**

Syntax Description

session -number	SS7 session number. Valid values are 0 and 1. You must enter the hyphen, with no space following it, after the **session** keyword.
segments	Maximum number of segments that the remote (Cisco IOS software) end can send before receiving an acknowledgment. Range is from 1 to 64. Default is 32.

Command Default

32 segments

Command Modes

Global configuration(config)

Command History

Release	Modification
12.0(7)XR	This command was introduced.
12.1(1)T	This command was integrated into Cisco IOS Release 12.1(1)T.

Usage Guidelines

Caution Use the default setting. Do not change session timers unless instructed to do so by Cisco technical support. Changing timers may result in service interruption or outage.

The outstanding segments counter is the maximum number of segments that the Cisco IOS software end of the connection can send without getting an acknowledgment from the receiver. The receiver uses the counter for flow control.

Examples

The following example sets up two sessions and for each session sets a maximum of 36 segments for receipt before an acknowledgment:

```
ss7 session-0 address 255.255.255.251 7000 255.255.255.254 7001
ss7 session-0 m_rcvnum 36
ss7 session-1 address 255.255.255.253 7002 255.255.255.254 7000
ss7 session-1 m_rcvnum 36
```

Related Commands

Command	Description
show ss7	Displays the SS7 configuration.

Command	Description
ss7 session cumack_t	Sets the cumulative acknowledgment timer.
ss7 session k_pt	Sets the null segment (keepalive) timer.
ss7 session m_cumack	Sets the maximum number of segments that can be received before the RUDP sends an acknowledgment.
ss7 session m_outseq	Sets the maximum number of out-of-sequence segments that can be received before the RUDP sends an extended acknowledgment.
ss7 session m_retrans	Sets the maximum number of times that the Reliable User Datagram Protocol (RUDP) attempts to resend a segment before declaring the connection invalid.
ss7 session retrans_t	Sets the retransmission timer.

ss7 session m_retrans

To set the maximum number of times that the Reliable User Datagram Protocol (RUDP) attempts to resend a segment before declaring the connection invalid in a specific SS7 signaling link session, use the **ss7 session m_retrans** command in global configuration mode. To reset to the default, use the **no** form of this command.

ss7 session-session *number* **m_retrans** *number*
no ss7 session-session *number* **m_retrans**

Syntax Description

session-number	SS7 session number. Valid values are 0 and 1. You must enter the hyphen, with no space following it, after the **session** keyword.
number	Maximum number of times that the RRUDP attempts to resend a segment before declaring the connection broken. Range is from 0 to 255. Default is 2.

Command Default

2 times

Command Modes

Global configuration (config)

Command History

Release	Modification
12.0(7)XR	This command was introduced.
12.1(1)T	This command was integrated into Cisco IOS Release 12.1(1)T.

Usage Guidelines

Caution Use the default setting. Do not change session timers unless instructed to do so by Cisco technical support. Changing timers may result in service interruption or outage.

The retransmission counter is the number of times a segment has been retransmitted. If this counter reaches the configured maximum, the transmitter resets the connection and informs the upper-layer protocol.

If you set this parameter to 0, the RUDP attempts to resend the segment continuously.

Examples

The following example sets up two sessions and for each session sets a maximum number of three times to resend before a session becomes invalid:

```
ss7 session-0 address 255.255.255.251 7000 255.255.255.254 7001
ss7 session-0 m_retrans 3
ss7 session-1 address 255.255.255.253 7002 255.255.255.254 7000
ss7 session-1 m_retrans 3
```

Related Commands

Command	Description
show ss7	Displays the SS7 configuration.

Command	Description
ss7 session cumack_t	Sets the cumulative acknowledgment timer.
ss7 session k_pt	Sets the null segment (keepalive) timer.
ss7 session m_cumack	Sets the maximum number of segments that can be received before the RUDP sends an acknowledgment.
ss7 session m_outseq	Sets the maximum number of out-of-sequence segments that can be received before the RUDP sends an extended acknowledgment.
ss7 session m_rcvnum	Sets the maximum number of segments that the remote end can send before receiving an acknowledgment.
ss7 session retrans_t	Sets the retransmission timer.

ss7 session retrans_t

To set the amount of time that the Reliable User Datagram Protocol (RUDP) waits to receive an acknowledgment for a segment in a specific SS7 signaling link session, use the **ss7 session retrans_t**command in global configuration mode. If the RUDP does not receive the acknowledgment in this time period, the RUDP retransmits the segment. To reset to the default, use the **no** form of this command.

ss7 session-session *number* **retrans_t** *milliseconds*
no ss7 session-session *number* **retrans_t**

Syntax Description

session -number	SS7 session number. Valid values are 0 and 1. You must enter the hyphen, with no space following it, after the **session** keyword.
milliseconds	Amount of time, in milliseconds, that the RUDP waits to receive an acknowledgment for a segment. Range is from 100 to 65535. Default is 600.

Command Default

600 ms

Command Modes

Global configuration (config)

Command History

Release	Modification
12.0(7)XR	This command was introduced.
12.1(1)T	This command was integrated into Cisco IOS Release 12.1(1)T.

Usage Guidelines

Caution Use the default setting. Do not change session timers unless instructed to do so by Cisco technical support. Changing timers may result in service interruption or outage.

The retransmission timer is used to determine whether a packet must be retransmitted and is initialized each time a data, null, or reset segment is sent. If an acknowledgment for the segment is not received by the time the retransmission timer expires, all segments that have been transmitted--but not acknowledged--are retransmitted.

This value should be greater than the value configured for the cumulative acknowledgment timer by using the **ss7 session cumack_t**command.

Examples

The following example sets up two sessions and specifies 550 ms as the time to wait for an acknowledgment for each session:

```
ss7 session-0 address 255.255.255.251 7000 255.255.255.254 7001
ss7 session-0 retrans_t 550
ss7 session-1 address 255.255.255.253 7002 255.255.255.254 7000
ss7 session-1 retrans_t 550
```

Related Commands

Command	Description
show ss7	Displays the SS7 configuration.
ss7 session cumack_t	Sets the cumulative acknowledgment timer.
ss7 session k_pt	Sets the null segment (keepalive) timer.
ss7 session m_cumack	Sets the maximum number of segments that can be received before the RUDP sends an acknowledgment.
ss7 session m_outseq	Sets the maximum number of out-of-sequence segments that can be received before the RUDP sends an extended acknowledgment.
ss7 session m_rcvnum	Sets the maximum number of segments that the remote end can send before receiving an acknowledgment.
ss7 session m_retrans	Sets the maximum number of times that the RUDP attempts to resend a segment before declaring the connection invalid.

ss7 set

Note Effective with Cisco IOS Release 12.2(15)T, the **ss7 set** command replaces the ss7 set failover-timer command.

To independently select failover-timer values for each session set and to specify the amount of time that the SS7 Session Manager waits for the active session to recover or for the standby media gateway controller (MGC) to indicate that the Cisco Signaling Link Terminal (SLT) should switch traffic to the standby session, use the **ss7 set**command in global configuration mode. To restore the failover timer to its default value of 5, use the **no** form of this command.

ss7 set [**session-set** *session-id*] **failover-timer** *ft-value*
no ss7 set [**session-set** *session-id*] **failover-timer**

Syntax Description

session-set *session-id*	(Optional) Selects failover timer values for each SS7 session set. Valid values are from 1 to 5. Default is 0.
failover -timer *ft-value*	Time, in seconds, that the Session Manager waits for a session to recover. Valid values range from 1 to 10. Default is 5.

Command Default

The failover timer is not set.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(15)T	This command was introduced. This command replaces the **ss7 set failover-timer**command.

Usage Guidelines

The failover-timer keyword and the ft-value argument specify the number of seconds that the Session Manager waits for the active session to recover or for the standby MGC to indicate that the SLT should switch traffic to the standby session and to make that session the active session. If the failover timer expires without recovery of the original session or if the system fails to get an active message from the standby MGC, the signaling links are taken out of service.

The no form of this command restores the failover timer to its default value of 5. Omitting the optional session-set keyword implicitly selects SS7 session set 0, which is the default.

Examples

The following example sets the failover timer to four seconds without using the session-set option:

```
ss7 set failover-timer 4
```

The following example sets the failover timer to 10 seconds and sets the SS7 session set value to 5:

```
ss7 set session-set 5 failover-timer 10
```

Related Commands

Command	Description
ss7 session	Creates a Reliable User Datagram Protocol (RUDP) session and explicitly adds an RUDP session to a Signaling System 7 (SS7) session set.
ss7 set failover timer	Specifies the amount of time that the Session Manager waits for the session to recover before declaring the session inactive.

ss7 set failover-timer

To specify the amount of time that the SS7 Session Manager waits for the active session to recover or for the standby Media Gateway Controller to indicate that the SLT should switch traffic to the standby session, use the **ss7 set failover-timer**command in global configuration mode. To reset ti the default, use the **no** form of this command.

ss7 set failover-timer [*seconds*]
no ss7 set failover-timer

Syntax Description

seconds	Time, in seconds, that the session manager waits for a session to recover. Range is from 1 to 10. Default is 3.

Command Default

3 seconds

Command Modes

Global configuration (config)

Command History

Release	Modification
12.0(7)XR	This command was introduced.
12.1(1)T	This command was integrated into Cisco IOS Release 12.1(1)T.

Usage Guidelines

This command specifies the number of seconds that the session manager waits for the active session to recover or for the standby media gateway controller to indicate that the SLT should switch traffic to the standby session and to make that session the active session. If the timer expires without a recovery of the original session or an active message from the standby media gateway controller, the signaling links are taken out of service.

Examples

The following example sets the failover timer to 4 seconds:

```
ss7 set failover-timer 4
```

Related Commands

Command	Description
show ss7 sm set	Displays the current failover timer setting.
ss7 session	Establishes a session.

station-id name

To specify the name that is to be sent as caller ID information and to enable caller ID, use the **station-id name** command in voice-port configuration mode at the sending Foreign Exchange Station (FXS) voice port or at a Foreign Exchange Office (FXO) port through which routed caller ID calls pass. To remove the name, use the **no** form of this command.

station-id name *name*
no station-id name *name*

Syntax Description

name	Station-id name. Must be a string of 1 to 15 characters.

Command Modes

The default is no station-id name.

Command Modes

Voice-port configuration (config-voiceport)

Command History

Release	Modification
12.1(2)XH	This command was introduced on the Cisco 2600 series, Cisco 3600 series, and Cisco MC3810.
12.1(3)T	This command was integrated into Cisco IOS Release 12.1(3)T.

Usage Guidelines

This optional command is configured on FXS voice ports that are used to originate on-net calls. The information entered is displayed by the telephone attached to the FXS port at the far end of the on-net call. It can also be configured on the FXO port of a router on which caller ID information is expected to be received from the Central Office (CO), to suit situations in which a call is placed from the CO, then goes through the FXO interface, and continues to a far-end FXS port through an on-net call. In this case, if no caller ID information is received from the CO telephone line, the far-end call recipient receives the information configured on the FXO port.

Note This feature applies only to caller ID name display provided by an FXS port connection to a telephone device. The station-id name is not passed through telephone trunk connections supporting Automatic Number Identification (ANI) calls. ANI supplies calling number identification only and does not support calling number names.

Do not use this command when the caller ID standard is dual-tone multifrequency (DTMF). DTMF caller ID can carry only the calling number.

If the **station-id name**, **station-id number**, or a **caller-id alerting**command is configured on the voice port, caller ID is automatically enabled, and the **caller-id enable**command is not necessary.

Examples

The following example configures a voice port from which caller ID information is sent:

```
voice-port 1/0/1
 cptone US
 station-id name A. Person
```

```
 station-id number 4085550111
Router(config-voiceport)#station-id
 ?
  name    A string describing station-id name
  number  A full E.164 telephone number
```

Related Commands

Command	Description
caller -id enable	Enables caller ID operation.
station-id number	Enables caller ID operation and specifies the number sent from the originating station-id or network FXO port for caller ID purposes.

station-id number

To specify the telephone or extension number that is to be sent as caller ID information and to enable caller ID, use the **station-id number** command in voice-port configuration mode at the sending Foreign Exchange Station (FXS) voice port or at a Foreign Exchange Office (FXO) port through which routed caller ID calls pass. To remove the number, use the **no** form of this command.

station-id number *number*
no station-id number *number*

Syntax Description

number	Station-id number. Must be a string of 1 to 15 characters.

Command Default

The default is no station-id number.

Command Modes

Voice-port configuration (config-voiceport)

Command History

Release	Modification
12.1(2)XH	This command was introduced on the Cisco 2600 series, Cisco 3600 series, and Cisco MC3810.
12.1(3)T	This command was integrated into Cisco IOS Release 12.1(3)T.

Usage Guidelines

This optional command is configured on FXS voice ports that are used to originate on-net calls. The information entered is displayed by the telephone attached to the FXS port at the far end of the on-net call. It can also be configured on the FXO port of a router on which caller ID information is expected to be received from the Central Office (CO), to suit situations in which a call is placed from the CO, then goes through the FXO interface, and continues to a far-end FXS port through an on-net call. In this case, if no caller ID information is received from the CO telephone line, the far-end call recipient receives the information configured on the FXO port.

Within the network, if an originating station-id does not include configured number information, Cisco IOS software determines the number by using reverse dial-peer search.

Note This feature applies only to caller ID name display provided by an FXS port connection to a telephone device. The station-id name is not passed through telephone trunk connections supporting Automatic Number Identification (ANI) calls. ANI supplies calling number identification only and does not support calling number names.

If the **station-id name**, **station-id number**, or a **caller-id alerting**command is configured on the voice port, caller ID is automatically enabled, and the **caller-id enable**command is not necessary.

Examples

The following example configures a voice port from which caller ID information is sent:

```
voice-port 1/0/1
 cptone US
 station-id name A. Person
```

```
 station-id number 4085550111
Router(config-voiceport)#station-id
 ?
  name    A string describing station-id name
  number  A full E.164 telephone number
```

Related Commands

Command	Description
caller -id enable	Enables caller ID operation.
station-id name	Enables caller ID operation and specifies the name sent from the originating station-id or network FXO port for caller ID purposes.

stats

To enable statistics collection for voice applications, use the **stats** command in application configuration monitor mode. To reset to the default, use the **no** form of this command.

stats
no stats

Syntax Description

This command has no arguments or keywords.

Command Default

Statistics collection is disabled.

Command Modes

Application configuration monitor

Command History

Release	Modification
12.3(14)T	This command was introduced to replace the **call application stats** command.

Usage Guidelines

To display the application statistics, use the **show call application session-level**, **show call application app-level**, or **show call application gateway-level**command. To reset the application counters in history to zero, use the **clear call application stats** command.

Examples

The following example enables statistics collection for voice applications:

```
application
monitor
stats
```

Related Commands

Command	Description
call application interface stats	Enables statistics collection for application interfaces.
call application stats	Enables statistics collection for voice applications.
clear call application stats	Clears application-level statistics in history and subtracts the statistics from the gateway-level statistics.
clear call application stats	Clears application-level statistics in history and subtracts the statistics from the gateway-level statistics.
interface stats	Enables statistics collection for application interfaces.
show call application app-level	Displays application-level statistics for voice applications.
show call application gateway-level	Displays gateway-level statistics for voice application instances.
show call application session-level	Displays event logs and statistics for voice application instances.

stcapp

To enable the SCCP Telephony Control Application (STCAPP), use the **stcapp** command in global configuration mode. To disable the STCAPP, use the **no** form of this command.

stcapp
no stcapp

Syntax Description

This command has no arguments or keywords.

Command Default

The Cisco CallManager does not control Cisco IOS gateway-connected analog and BRI endpoints.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.3(14)T	This command was introduced.

Usage Guidelines

Use the **stcapp**command to enable basic Skinny Client Call Control (SCCP) call control features for BRI and foreign exchange stations (FXS) analog ports within Cisco IOS voice gateways. The **stcapp**command enables the Cisco IOS gateway application to support the following features:

- Line-side support for the Multilevel Precedence and Preemption (MLPP) feature
- Cisco CallManager registration of analog and Basic Rate Interface BRI endpoints
- Cisco CallManager endpoint autoconfiguration support
- Modem pass-through support
- Cisco Survivable Remote Site Telephony (SRST) support

Examples

The following example shows that STCAPP is enabled:

```
Router(config)# stcapp
```

Related Commands

Command	Description
ccm-manager config server	Specifies the TFTP server for SCCP gateway downloads.
ccm-manager sccp local	Specifies the SCCP local interface for Cisco CallManager registration.
sccp	Enables the SCCP protocol.
show stcapp device	Displays configuration information about STCAPP) voice ports.
show stcapp statistics	Displays call statistics for STCAPP voice ports.
stcapp ccm-group	Configures the Cisco CallManager group number for use by the STCAPP.

Command	Description
stcapp timer	Enables STCAPP timer configuration.

stcapp call-control mode

To configure call control mode for Skinny Client Control Protocol (SCCP) gateway supplementary features, use the **stcapp call-control mode** command in global configuration mode. To disable call control mode, use the **no** form of this command

stcapp call-control mode [**feature** | **standard**]
no stcapp call-control mode [**feature** | **standard**]

Syntax Description

feature	(Optional) Feature mode call control.
standard	(Optional) Standard mode call control. This is the default.

Command Default

Standard mode call control is enabled.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.4(6)XE	This command was introduced.
12.4(11)T	This command was integrated into Cisco IOS Release 12.4(11)T.

Usage Guidelines

This command enables feature mode call control, which allows SCCP analog phone users to invoke a feature by dialing a feature access code (FAC). The following table lists the features and FACs that you can use in feature mode.

Feature	FAC
Drop Last Active Call	#1
Call Transfer	#2
Call Conference	#3
Drop Last Conferee	#4
Toggle Between Two Calls	#5

Examples

The following partial output from the **show running-config** command shows feature call control mode enabled:

```
Router# show running-config
.
.
.
stcapp call-control mode feature
!
```

The following partial output from the **show running-config** command shows standard call control mode enabled:

```
Router# show running-config
.
.
.
stcapp call-control mode standard
!
!
```

Related Commands

Command	Description
show stcapp feature codes	Displays current values for SCCP telephony control (STC) application feature access codes.

stcapp feature callback

To enable CallBack on Busy and enter the STC application feature callback configuration mode, use the **stcapp feature callback** command in global configuration mode. To disable the feature in the STC application, use the **no** form of this command.

stcapp feature callback
no stcapp feature callback

Syntax Description

This command has no arguments or keywords.

Command Default

CallBack on Busy in the STC application is disabled.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.4(20)YA	This command was introduced.
12.4(22)T	This command was integrated into Cisco IOS Release 12.4(22)T.

Usage Guidelines

This command enables CallBack on Busy and enters the STC application feature callback configuration mode for modifying the default values of the callback activation key and timer for CallBack on Busy.

Examples

The following example shows how to enable CallBack on Busy in the STC application:

```
Router(config)# stcapp feature callback
Router(config-stcapp-callback)#
```

Related Commands

Command	Description
activation-key	Defines the activation key for CallBack on Busy.
ringing-timeout	Defines the timeout period for CallBack on Busy.

stcapp ccm-group

To configure the Cisco CallManager group number for use by the SCCP Telephony Control Application (STCAPP), use the **stcapp ccm-group** command in global configuration mode. To disable STCAPP Cisco CallManager group number configuration, use the **no** form of this command.

stcapp ccm-group *group-id*
no stcapp ccm-group *group-id*

Syntax Description

group-id	Cisco CallManager group number.

Command Default

No Cisco CallManager group number is configured.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.3(14)T	This command was introduced.

Usage Guidelines

The Cisco CallManager group identifier must have been configured for the service provider interface (SPI) using the **sccp ccm-group** *group-id*command.

Examples

The following example configures the STCAPP to use Cisco CallManager group 2:

```
Router(config)# stcapp ccm-group 2
```

Related Commands

Command	Description
show stcapp device	Displays configuration information about SCCP Telephony Control Application (STCAPP) voice ports.
show stcapp statistics	Displays call statistics for SCCP Telephony Control Application (STCAPP) voice ports.
stcapp	Enables the SCCP Telephony Control Application (STCAPP).
stcapp timer	Enables SCCP Telephony Control Application (STCAPP) timer configuration.

stcapp feature access-code

To enable feature access codes (FACs) in the STC application and enter the STC application feature access-code configuration mode, use the **stcapp feature access-code** command in global configuration mode. To disable the use of all STC application feature access codes, use the **no** form of this command.

stcapp feature access-code
no stcapp feature access-code

Syntax Description

This command has no arguments or keywords.

Command Default

All feature access codes are disabled.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.4(2)T	This command was introduced.

Usage Guidelines

This command enables feature access codes (FACs) in the SCCP telephony control (STC) application and enters the STC application feature access-code configuration mode to modify the default values of the prefix and feature codes for FACs.

The **no** form of this command blocks the use of FACs on all analog ports.

Use the **show stcapp feature codes** command to display a list of all FACs.

Examples

The following example shows how to enable FACs in the STC application.

```
Router(config)# stcapp feature access-code
Router(stcapp-fac)#
```

Related Commands

Command	Description
call forward all	Defines the feature code in the feature access code (FAC) for forwarding all calls.
call forward cancel	Defines the feature code in the feature access code (FAC) for cancelling Call Forward All.
pickup direct	Defines the feature code in the feature access code (FAC) for Directed Call Pickup.
pickup group	Defines the feature code in the feature access code (FAC) for call pickup from another group.
pickup local	Defines the feature code in the feature access code (FAC) for call pickup from the local group.

Command	Description
prefix (stcapp-fac)	Defines the prefix for feature access codes (FACs).
show stcapp feature codes	Displays all feature access codes (FACs).

stcapp feature callback

To enable CallBack on Busy and enter the STC application feature callback configuration mode, use the **stcapp feature callback** command in global configuration mode. To disable the feature in the STC application, use the **no** form of this command.

stcapp feature callback
no stcapp feature callback

Syntax Description

This command has no arguments or keywords.

Command Default

CallBack on Busy in the STC application is disabled.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.4(20)YA	This command was introduced.
12.4(22)T	This command was integrated into Cisco IOS Release 12.4(22)T.

Usage Guidelines

This command enables CallBack on Busy and enters the STC application feature callback configuration mode for modifying the default values of the callback activation key and timer for CallBack on Busy.

Examples

The following example shows how to enable CallBack on Busy in the STC application:

```
Router(config)# stcapp feature callback
Router(config-stcapp-callback)#
```

Related Commands

Command	Description
activation-key	Defines the activation key for CallBack on Busy.
ringing-timeout	Defines the timeout period for CallBack on Busy.

stcapp feature speed-dial

To enable STC application feature speed-dial codes and enter their configuration mode, use the **stcapp feature speed-dial** command in global configuration mode. To disable the use of all STC application feature speed-dial codes, use the **no** form of this command.

stcapp feature speed-dial
no stcapp feature speed-dial

Syntax Description

This command has no arguments or keywords.

Command Default

All feature speed-dial codes are disabled.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.4(2)T	This command was introduced.

Usage Guidelines

This command is used with the SCCP telephony control (STC) application, which enables certain features on analog FXS endpoints that use Skinny Client Control Protocol (SCCP) for call control.

Although feature speed-dial (FSD) prefixes and codes for analog FXS ports are configured on the voice gateway that has the FXS ports, the actual numbers that are dialed using these codes are configured on Cisco CallManager or the Cisco CallManager Express system.

The **no** form of this command blocks the use of FSD codes on all analog ports.

Note that all the STC FSD codes have defaults. To return codes under this configuration mode to their defaults, you must use the **no** form of the individual commands one at a time.

Examples

The following example sets an FSD prefix of three asterisks (***) and speed-dial codes from 2 to 7. After these values are configured, a phone user presses ***2 on the keypad to speed-dial the telephone number that is stored with speed-dial 1 on the call-control system (Cisco CallManager or Cisco CallManager Express).

```
Router(config)# stcapp feature speed-dial
Router(stcapp-fsd)# prefix ***
Router(stcapp-fsd)# speed dial from 2 to 7
Router(stcapp-fsd)# redial 9
Router(stcapp-fsd)# voicemail 8
Router(stcapp-fsd)# exit
```

The following example shows how the speed-dial range that is set in the example above is mapped to the speed-dial positions on the call-control system. Note that the range from 2 to 7 is mapped to speed-dial 1 to 6.

```
Router# show stcapp feature codes
.
.
.
```

```
stcapp feature speed-dial
  prefix ***
  redial ***9
  voicemail ***8
  speeddial1 ***2
  speeddial2 ***3
  speeddial3 ***4
  speeddial4 ***5
  speeddial5 ***6
  speeddial6 ***7
```

Related Commands

Command	Description
prefix (stcapp-fsd)	Designates a prefix to precede the dialing of an STC application feature speed-dial code.
redial	Designates an STC application feature speed-dial code to dial again the last number that was dialed.
show stcapp feature codes	Displays configured and default STC application feature codes.
speed dial	Designates a range of STC application feature speed-dial codes.
voicemail (stcapp-fsd)	Designates an STC application feature speed-dial code to dial the voice-mail number.

stcapp register capability

To specify modem capability for SCCP Telephony Control Application (STCAPP) devices, use the **stcapp register capability**command in global configuration mode. To disable modem capability, use the **no** form of this command.

stcapp register capability *voice-port* [**both** | **modem-passthrough** | **modem-relay**]
no stcapp register capability *voice-port*

Syntax Description

voice-port	Voice interface slot number 1 through 4
both	Specifies support for both modem-relay and modem pass-through.
modem - passthrough	Specifies support for modem pass-through.
modem - relay	Specifies support for V.150.1 modem relay.

Command Default

No voice port modem capability is enabled.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.4(4)T	This command was introduced.

Usage Guidelines

Use the **stcapp register capability** *command to specify modem transport methods for STCAPP-controlled devices registering with Cisco Call-Manager. If this command is applied while the voice port is idle, the port automatically reregisters with the Cisco CallManager. If there is an active call on the voice port when this command is applied, the port does not reregister.*Although Cisco does not recommend the procedure, to force device reregistration you must either manually shut down the device using the **shutdown** command in voice-port configuration mode, or reset it from the Cisco CallManager.

Use the voice service configuration command **modem passthrough** to globally enable modem pass-through capability, thereby providing fallback to voice band data (modem pass-through) when the voice gateway communicates with a Secure Telephone Unit (STU) or nonmodem-relay capable gateway.

Examples

The following example configures the device connected to voice port 1/1/0 to support both modem capabilities:

```
Router(config)# stcapp register capability 1/1/0 both
```

Related Commands

Command	Description
modem passthrough	Globally enables modem pass-through over VoIP.
show stcapp device voice-port	Displays configuration information for STCAPP devices.

Command	Description
shutdown	Disables voice ports on the VIC.

stcapp security mode

To enable security for Skinny Client Control Protocol (SCCP) Telephony Control Application (STCAPP) endpoints and specify the security mode to be used for setting up the Transport Layer Security (TLS) connection, use the **stcapp security mode** command in global configuration mode. To disable security for the endpoint, use the no form of this command.

stcapp security mode [**authenticated** | **encrypted** | **none**]
no stcapp security

Syntax Description

mode	Sets the global security mode for all STCAPP endpoints.
authenticated	Sets the security mode to authenticated and enables SCCP signaling between the voice gateway and Cisco Unified CME through the secure TLS connection on TCP port 2443.
encrypted	Sets the security mode to encrypted and enables SCCP signaling between the voice gateway and Cisco Unified CME to take place through Secure Real-Time Transport Protocol (SRTP).
none	Sets the security mode to none (Default).

Command Default

Security is not enabled.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.4(11)XW1	This command was introduced.
12.4(20)T	This command was integrated into Cisco IOS Release 12.4(20)T.

Usage Guidelines

You must enter both the **stcapp security mode**and **stcapp security trustpoint** commands to enable security for the STCAPP end point. The **stcapp security trustpoint** command must be configured for the STCAPP service to start.

SCCP signaling security mode can be set for each dial peer using the **security mode** command in dial peer configuration mode. If you use both the **stcapp security mode** and the **security mode**commands, the dial-peer level command, **security mode**, overrides the global setting.

Examples

The following example configures STCAPP security mode with the trustpoint mytrustpoint:

```
Router(config)# stcapp ccm-group 1
Router(config)# stcapp security mytrustpoint
Router(config)# stcapp security mode encrypted
Router(config)# stcapp
```

Related Commands

Command	Description
security mode	Sets the security mode for a specific dial peer using STCAPP services in a secure Cisco Unified CME network.
stcapp	Enables the STCAPP.
stcapp ccm-group	Configures the Cisco Unified Communications Manager group number for use by the STCAPP.
stcapp security trustpoint	Enables security for STCAPP endpoints and specifies the trustpoint for setting up the TLS connection.

stcapp security trustpoint

To enable security for Skinny Client Control Protocol (SCCP) Telephony Control Application (STCAPP) endpoints and specify the trustpoint to be used for setting up the Transport Layer Security (TLS) connection, use the **stcapp security** command in global configuration mode. To disable security for the endpoint and delete all identity information and certificates associated with the trustpoint, use the no form of this command.

stcapp security trustpoint *line*
no stcapp security

Syntax Description

trustpoint	Security trustpoint label for all STCAPP endpoints.
line	Text description that identifies the trustpoint.

Command Default

Security is not enabled and no trustpoint is specified.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.4(11)XW1	This command was introduced.
12.4(20)T	This command was integrated into Cisco IOS Release 12.4(20)T.

Usage Guidelines

You must enter both the **stcapp security mode**and **stcapp security trustpoint** commands to enable security for the STCAPP endpoint. The **stcapp security trustpoint** command must be configured for the STCAPP service to start. The trustpoint configured by this command contains the device certificate and must match the trustpoint configured on the router using the **crypto pki trustpoint** command. All analog phones use the same certificate. Cisco Unified Communications Manager Express does not require a different certificate for each phone.

Examples

The following example configures STCAPP security mode with the trustpoint mytrustpoint:

```
Router(config)# stcapp ccm-group 1
Router(config)# stcapp security mytrustpoint
Router(config)# stcapp security mode encrypted
Router(config)# stcapp
```

Related Commands

Command	Description
crypto pki trustpoint	Declares the trustpoint that your router should use.
stcapp ccm-group	Configures the Cisco Unified Communications Manager group number for use by the STCAPP.
stcapp	Enables the STCAPP.

Command	Description
stcapp security mode	Enables security for STCAPP endpoints and specifies the security mode to be used for setting up the TLS connection.

stcapp supplementary-services

To enter supplementary-service configuration mode for configuring STC application supplementary-service features on an FXS port, use the **stcapp supplementary-services** command in global configuration mode. To remove the configuration, use the **no** form of this command.

stcapp supplementary-services
no stcapp supplementary-services

Syntax Description

This command has no arguments or keywords.

Command Default

No configuration for STC application supplementary-service features exists.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.4(20)YA	This command was introduced.
12.4(22)T	This command was integrated into Cisco IOS Release 12.4(22)T.

Usage Guidelines

This command enters the supplementary-service configuration mode for configuring STC application supplementary-service features for analog FXS ports on a Cisco IOS voice gateway, such as a Cisco integrated services router (ISR) or Cisco VG224 Analog Phone Gateway.

Examples

The following example shows how to enable the Hold/Resume STC application supplementary-service feature for analog phones connected to port 2/0 on a Cisco VG224.

```
Router(config)# stcapp supplementary-services
Router(config-stcapp-suppl-serv)# port 2/0
Router(config-stcapp-suppl-serv-port)# hold-resume
Router(config-stcapp-suppl-serv-port)# end
```

Related Commands

Command	Description
port (supplementary-service)	Specifies analog FXS port on which STC application supplementary-service features are to be supported.

stcapp timer

To enable SCCP Telephony Control Application (STCAPP) timer configuration, use the **stcapp timer**command in global configuration mode. To disable STCAPP timer configuration, use the **no** form of this command.

stcapp timer roh *seconds*
no stcapp timer

Syntax Description

roh	Receiver off hook (ROH) tone timeout.
seconds	Duration, in seconds, that the receiver off-key tone is played. Range is 0 to 120 seconds.

Command Default

seconds: 45 seconds

Command Modes

Global configuration (config)

Command History

Release	Modification
12.3(14)T	This command was introduced.

Usage Guidelines

Use this command to configure the STCAPP ROH timer for the maximum time that ROH tone is played. ROH tone signals a subscriber that the phone remains off hook when there is no active call.

Examples

The following example configures the receiver off hook timer for 30 seconds:

```
Router(config)# stcapp timer roh 30
```

Related Commands

Command	Description
show call application voice stcapp	Displays information about the STCAPP.
stcapp	Enables the STCAPP.

stream-service profile

To associate details specific to stream service with the media class on CUBE, use the **stream-service profile** *tag* command in media class configuration mode. To revert the stream service association, use the **no** form of this command.

stream-service profile *tag*
no stream-service profile *tag*

Syntax Description

tag	The stream-service profile tag. Range is 1–10000.

Command Default

Stream service profile isn't associated with the media class by default.

Command Modes

Media Class configuration mode (cfg-mediaclass)

Command History

Release	Modification
Cisco IOS XE Bengaluru 17.6.1a	This command was introduced on Cisco Unified Border Element.

Usage Guidelines

The **stream-service profile** *tag* command associates a stream service profile with a media class. This profile is then configured in **media profile stream-service** *tag* command to enable stream-service in CUBE.

Examples

The following is a sample configuration for stream-service profile in CUBE:

```
router(config)#media class 9
csr(cfg-mediaclass)#stream-service ?
profile select media profile stream-service

csr(cfg-mediaclass)#stream-service profile ?
<1-10000> media profile stream-service tag

csr(cfg-mediaclass)#stream-service profile 99
```

Related Commands

Command	Description
media profile stream-service	Enables stream service on CUBE.
connection (media-profile)	Configures idle timeout and call threshold for a media profile.
proxy (media-profile)	Configures IP address or hostname of proxy in media profile.
source-ip (media-profile)	Configures local source IP address of a WebSocket connection.
media class	Applies the media class at the dial peer level.

stun

To enter STUN configuration mode for configuring firewall traversal parameters, use the **stun** command in voice-service voip configuration mode. To remove stun parameters, use the **no** form of this command.

stun
no stun

Syntax Description

This command has no arguments or keywords.

Command Default

No default behavior or values.

Command Modes

Voice-service voip configuration (config-voi-serv).

Command History

Release	Modification
12.4(22)T	This command was introduced.
Cisco IOS XE Cupertino 17.7.1a	Introduced support for YANG models.

Usage Guidelines

Use this command to enter the configuration mode to configure firewall traversal parameters for VoIP communications.

Examples

The following example shows how to enter STUN configuration mode.

```
Router(config)#voice service voip
Router(config-voi-serv)#stun
```

Related Commands

Command	Description
stun flowdata agent-id	Configures the agent ID.
stun flowdata keepalive	Configures the keepalive interval.
stun flowdata shared-secret	Configures a secret shared between call control agent and firewall.
stun usage firewall-traversal flowdata	Enables firewall traversal using stun.
voice-class stun-usage	Enables firewall traversal for VoIP communications.

stun flowdata agent-id

To configure the stun flowdata agent ID, use the **stun flowdata agent-id**command in STUN configuration mode. To return to the default value for agent ID, use the **no** form of this command.

stun flowdata agent-id *tag* [*boot-count*]
no stun flowdata agent-id *tag* [*boot-count*]

Syntax Description

tag	Unique identifier in the range 0 to 255. Default is -1.
boot-count	(Optional) Value of boot-count. Range is 0 to 65535. Default is zero.

Command Default

No firewall traversal is performed.

Command Modes

STUN configuration (conf-serv-stun)

Command History

Release	Modification
12.4(22)T	This command was introduced.

Usage Guidelines

Use the **stun flowdata agent-id**command to configure the agent id and the boot count to configure call control agents which authorize the flow of traffic.

Configuring the boot-count keyword helps to prevent anti-replay attacks after the router is reloaded. If you do not configure a value for boot count, the boot-count is initialized to 0 by default. After it is initialized, it is incremented by one automatically upon each reboot and the value saved back to NVRAM. The value of boot count is reflected in **show running** configuration command.

Examples

The following example shows how the **stun flowdata agent-id** command is used at the router prompt.

```
Router#enable
Router#configure terminal
Router(config)#voice service voip
Router(conf-voi-serv)#stun
Router(conf-serv-stun)#stun flowdata agent-id 35 100
```

Related Commands

Command	Description
stun flowdata keepalive	Configures the keepalive interval.
stun flowdata shared-secret	Configures a secret shared between call control agent and firewall.

stun flowdata catlife

To configure the lifetime of the CAT, use the **stun flowdata catlife** command in STUN configuration mode. To return to the default catlife value, use the **no** form of this command.

stun flowdata catlife *liftetime* **keepalive** *interval*
no stun flowdata catlife *liftetime* **keepalive** *interval*

Syntax Description

liftetime	Lifetime of the CAT in seconds. The default value is 1270 (21 min 10 sec).
interval	Keepalive interval time in seconds. Range is 10 to 30. Default is 10.

Command Default

The default keepalive value is 10 seconds.

Command Modes

STUN configuration (conf-serv-stun)

Command History

Release	Modification
15.0(1)M	This command was introduced.

Usage Guidelines

Use the **stun flowdata catlife**command to configure call control agents which authorize the flow of traffic.

Examples

The following example shows how the **stun flowdata catlife** command is used at the router prompt.

```
Router(config)#voice service voip
Router(conf-voi-serv)#stun
Router(conf-serv-stun)#stun flowdata catlife 150 keepalive 30
```

Related Commands

Command	Description
stun	Enters stun configuration mode.
stun flowdata shared-secret	Configures a secret shared between call control agent and firewall.
stun flowdata agent-id	Configures the agent ID.

stun flowdata keepalive

Note Effective with Cisco IOS Release 15.0(1)M, the **stun flowdata keepalive** command is replaced by the command **stun flowdata catlife**.

To configure the keepalive interval, use the **stun flowdata keepalive** command in STUN configuration mode. To return to the default keepalive value, use the **no** form of this command.

stunflowdata keepalive *seconds*
no stunflowdata keepalive *seconds*

Syntax Description

seconds	Keepalive interval in seconds. Range is 1 to 65535. Default is 10.

Command Default

The default keepalive value is 10 seconds.

Command Modes

STUN configuration (conf-serv-stun)

Command History

Release	Modification
12.4(22)T	This command was introduced.
15.0(1)M	This command was replaced. The call application **stun flowdata keepalive** command was replaced by the commands **stun flowdata catlife**. The **stun flowdata keepalive** command is hidden and depreciated in Cisco IOS Release 15.0(1)M.

Usage Guidelines

You can use the **stun flowdata keepalive** command to decide how often to send keepalives. Keepalives are application mechanisms for maintaining alive the firewall traversal mappings associated with firewalls.

TRP works with a Call Agent which supports firewall traversal. In this mode, the Call Agent sends a request to TRP to open the pinhole. The request contains local, remote IP /Port, token, and other Cisco-flow data parameters.

TRP sends a STUN indication message to the firewall with Cisco-flow data, after processing the request. The message contains the STUN header, STUN username, and Cisco-flow data. The firewall validates the token in Cisco-flow data after receiving the STUN packet, and opens the pinhole if validation is successful.

Keepalives in STUN flow between the UDP peers to ensure that the firewall keeps the pinholes open.

This command is hidden and depreciated in Cisco IOS Release 15.0(1)M release because the keepalive interval is configured along with stun flowdata catlife command. When this command is configured or present in start-up configuration during reload, the following command will be nvgen'ed and displayed in **show run** command.

In addition, the following message will be printed during the configuration/reload:

```
Deprecated command. Setting catlife=1270 sec and keepalive=30 sec.
Use the following command to configure non-default values:
stun flowdata catlife <lifetime> keepalive <interval>
```

Examples

The following example shows how to change the **stun flowdata keepalive interval** from the default value (10) to 5 seconds.

```
Router(config)# voice service voip

Router(config-voi-serv)#stun
Router(config-serv-stun)#stun flowdata agent-id 35
Router(config-serv-stun)#stun flowdata shared-secret 123abc123abc
Router(config-serv-stun)#stun flowdata keepalive 5
```

Related Commands

Command	Description
stun	Enters stun configuration mode.
stun flowdata shared-secret	Configures a secret shared between call control agent and firewall.
stun flowdata agent-id	Configures the agent ID.

stun flowdata shared-secret

To configure a secret shared on a call control agent, use the **stun flowdata shared-secret** command in STUN configuration mode. To return the shared secret to the default value, use the **no** form of this command.

stun flowdata shared-secret tag *string*
no stun flowdata shared-secret

Syntax Description

tag	0--Defines the password in plaintext and will encrypt the password. 6-- Defines secure reversible encryption for passwords using type **6** Advanced Encryption Scheme (AES). **Note** Requires AES primary key to be preconfigured. 7-- Defines the password in hidden form and will validate the (encrypted) password before accepting it.
string	12 to 80 ASCII characters. Default is an empty string.

Command Default

The default value of this command sets the shared secret to an empty string. No firewall traversal is performed when the shared-secret has the default value.

Command Modes

STUN configuration (conf-serv-stun)

Command History

Release	Modification
12.4(22)T	This command was introduced.
15.0(1)M	This command was modified. The encryption values zero and seven was added to this command.
IOS XE 16.11.1a	Secure reversible encryption for passwords using type **6** Advanced Encryption Scheme (AES) was introduced.
Cisco IOS XE Dublin 17.10.1a	Introduced support for YANG models.

Usage Guidelines

A shared secret on a call control agent is a string that is used between a call control agent and the firewall for authentication purposes. The shared secret value on the call control agent and the firewall must be the same. This is a string of 12 to 80 characters. The **no** form of this command will remove the previously configured shared-secret if any. The default form of this command will set the shared-secret to NULL. The password can be encrypted and validated before it is accepted. Firewall traversal is not performed when the shared-secret is set to default.

It is mandatory to specify the encryption type for the shared secret. If a clear text password (type **0**) is configured, it is encrypted as type **6** before saving it to the running configuration.

If you specify the encryption for the shared secret as type **6** or **7**, the entered password is checked against a valid type **6** or **7** password format and saved as type **6** or **7** respectively.

Type-6 passwords are encrypted using AES cipher and a user-defined primary key. These passwords are comparatively more secure. The primary key is never displayed in the configuration. Without the knowledge of the primary key, type **6** shared secret passwords are unusable. If the primary key is modified, the password that is saved as type 6 is re-encrypted with the new primary key. If the primary key configuration is removed, the type **6** shared secret passwords cannot be decrypted, which may result in the authentication failure for calls and registrations.

Note When backing up a configuration or migrating the configuration to another device, the primary key is not dumped. Hence the primary key must be configured again manually.

To configure an encrypted preshared key, see Configuring an Encrypted Preshared Key.

Note The encryption type **7** is supported in IOS XE Release 16.11.1a, but will be deprecated in the later releases. Following warning message is displayed when encryption type **7** is configured.

```
Warning: Command has been added to the configuration using a type 7
password. However, type 7 passwords will soon be deprecated. Migrate to
a supported password type 6.
```

Examples

The following example shows how the **stun flowdata shared-secret** command is used.

```
Router(config)#voice service voip
Router(conf-voi-serv)#stun
Router(config-serv-stun)#stun flowdata shared-secret 6 123cisco123cisco
```

Related Commands

Command	Description
stun	Enters stun configuration mode.
stun flowdata agent-id	Configures the agent ID.
stun flowdata catlife	Configures the lifetime of the CAT.

stun usage firewall-traversal flowdata

To enable firewall traversal using stun, use the **stun usage firewall-traversal flowdata** command in voice class stun-usage configuration mode. To disable firewall traversal with stun, use the **no** form of this command.

stun usage firewall-traversal flowdata
no stun usage firewall-traversal flowdata

Syntax Description

This command has no arguments or keywords.

Command Default

Firewall traversal using STUN is not enabled.

Command Modes

Voice-class configuration (config-class)

Command History

Release	Modification
12.4(22)T	This command was introduced.
Cisco IOS XE Cupertino 17.7.1a	Introduced support for YANG models.

Examples

The following example shows how to enable firewall traversal using STUN:

```
Router(config)#voice class stun-usage 10
Router(config-class)#stun usage firewall-traversal flowdata
```

Related Commands

Command	Description
stun flowdata shared-secret	Configures a secret shared between call control agent and firewall.
voice class stun-usage	Configures a new voice class called stun-usage with a numerical tag.

stun usage ice lite

To enable ICE-lite using stun, use the **stun usage ice-lite** command in voice class stun-usage configuration mode. To disable ICE-lite with stun, use the **no** form of this command.

stun usage ice lite
no stun usage ice lite

Syntax Description

This command has no arguments or keywords.

Command Default

ICE-lite is not enabled by default.

Command Modes

Voice-class configuration (config-class)

Command History

Release	Modification
Cisco IOS XE 3.15S Cisco IOS 15.5(3)M	This command was introduced.

Examples

The following example shows how to enable ICE-lite using STUN:

```
Router(config)#voice class stun-usage 25
Router(config-class)#stun usage ice lite
```

subaddress

To configure a subaddress for a POTS port, use the **subaddress** command in dial-peer voice configuration mode. To disable the subaddress, use the **no** form of this command.

subaddress *number*
no subaddress *number*

Syntax Description

number	Actual subaddress of the POTS port.

Command Default

No subaddress is available for a POTS port.

Command Modes

Dial peer configuration (config-dial-peer)

Command History

Release	Modification
12.2(8)T	This command was introduced on the Cisco 803, Cisco 804, and Cisco 813.

Usage Guidelines

You can use this command for any dial-peer voice POTS port. You can configure only one subaddress for each of the POTS ports. The latest entered subaddress on the dial-peer voice port is stored. To check the status of the subaddress configuration, use the **show running-config** command.

Examples

The following examples show that a subaddress of 20 has been set for POTS port 1 and that a subaddress of 10 has been set for POTS port 2:

```
dial-peer voice 1 pots
 destination-pattern 5555555
 port 1
 no call-waiting
 ring 0
 volume 4
 caller-number 1111111 ring 3
 caller-number 2222222 ring 1
 caller-number 3333333 ring 1
 subaddress 20
dial-peer voice 2 pots
 destination-pattern 4444444
 port 2
 no call-waiting
 ring 0
 volume 2
 caller-number 6666666 ring 2
 caller-number 7777777 ring 3
 subaddress 10
```

subcell-mux

To enable ATM adaption layer 2 (AAL2) common part sublayer (CPS) subcell multiplexing on a Cisco router, use the **subcell-mux** command in voice-service configuration mode. To reset to the default, use the **no** form of this command.

subcell-mux *time*
no subcell-mux *time*

Syntax Description

time	Timer value, in milliseconds. Range is from 5 to 1000 (1 second). Default is 10.

Command Default

10 ms Subcell multiplexing is off

Command Modes

Voice-service configuration

Command History

Release	Modification
12.1(1)XA	This command was introduced on the Cisco MC3810.
12.1(2)T	This command was integrated into Cisco IOS Release 12.1(2)T.
12.2(2)XB	The *time* argument was implemented on the Cisco 3660.
12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T.

Usage Guidelines

Use thiscommand to enable ATM adaption layer 2 (AAL2) common part sublayer (CPS) subcell multiplexing when the Cisco router interoperates with other equipment that uses subcell multiplexing.

Examples

The following example sets AAL2 CPS subcell multiplexing to 15 ms:

```
Router(conf-voi-serv-sess)# subcell-mux 15
```

Related Commands

Command	Description
voice -service	Specifies the voice encapsulation type and enters voice-service configuration mode.

subscription asnl session history

To specify how long to keep Application Subscribe/Notify Layer (ASNL) subscription history records and how many history records to keep in memory, use the subscription asnl session history command in global configuration mode. To reset to the default, use the no form of this command.

subscription asnl session history {**count** *number* | **duration** *minutes*}
no subscription asnl session history {**count** | **duration**}

Syntax Description

count *number*	Number of records to retain in a session history.
duration *minutes*	Duration, in minutes, for which to keep the record.

Command Default

Default duration is 10 minutes. Default number of records is 50.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.3(4)T	This command was introduced.

Usage Guidelines

The ASNL layer maintains subscription information. Active subscriptions are retained in the active subscription table in system memory. When subscriptions are terminated, they are moved to the subscription table in system memory.

This command controls the ASNL history table. Use this command to specify how many minutes the history record is retained after the subscription is removed, and to specify how many records are retained at any given time.

Examples

The following example specifies that a total of 100 records are to be kept in the RTSP client history:

```
subscription asnl session history count 100
```

Related Commands

Command	Description
clear subscription	Clears all active subscriptions or a specific subscription.
debug asnl events	Traces event logs in the ASNL.
show subscription	Displays information about ASNL-based and non-ASNL-based SIP subscriptions.
subscription maximum	Specifies the maximum number of outstanding subscriptions to be accepted or originated by a gateway.

subscription maximum

To specify the maximum number of outstanding subscriptions to be accepted or originated by a gateway, use the subscription maximum command in voice service voip sip configuration mode. To remove the maximum number of subscriptions specified, use the **no** form of this command.

subscription maximum {**accept** | **originate**} *number*
no subscription maximum {**accept** | **originate**}

Syntax Description

accept	Subscriptions accepted by the gateway.
originate	Subscriptions originated by the gateway.
number	Maximum number of outstanding subscriptions to be accepted or originated by the gateway.

Command Default

The default number of subscriptions is equal to twice the number of dial-peers configured on the platform.

Command Modes

Voice service SIP configuration (conf-serv-sip)

Command History

Release	Modification
12.3(4)T	This command was introduced.

Usage Guidelines

Use this command to configure the maximum number of concurrent SIP subscriptions, up to twice the number of dial-peers configured.

Examples

The following example configures subscription maximums:

```
Router(config)# voice service voip
Router(conf-voi-serv)# sip
Router(conf-serv-sip)# subscription maximum originate 10
```

Related Commands

Command	Description
clear subscription	Clears all active subscriptions or a specific subscription.
retry subscribe	Configures the number of retries for SUBSCRIBE messages.
retry timer	Configures the retry interval for resending SIP messages.
show subscription	Displays active SIP subscriptions.

supervisory answer dualtone

To enable answer supervision on a Foreign Exchange Office (FXO) voice port, use the **supervisory answer dualtone command in**voice-port configuration mode. To disable answer supervision on a voice port, use the **no** form of this command.

supervisory answer dualtone [**sensitivity** {**high** | **medium** | **low**}]
no supervisory answer dualtone

Syntax Description

sensitivity	(Optional) Specific detection sensitivity for answer supervision.
high	Increased level of detection sensitivity.
medium	Default level of detection sensitivity.
low	Decreased level of detection sensitivity.

Command Default

Answer supervision is not enabled on voice ports.

Command Modes

Voice-port configuration (config-voiceport)

Command History

Release	Modification
12.2(2)T	This command was introduced on the following platforms: Cisco 1750, Cisco 2600 series, Cisco 3600 series, and Cisco MC3810.

Usage Guidelines

This command configures the FXO voice port to detect voice, fax, and modem traffic when calls are answered. If answer supervision is enabled, calls are not recorded as connected until answer supervision is triggered.

This command enables a ring-no-answer timeout that drops calls after a specified period of ringback. The period of ringback can be configured using the **timeouts ringing** command.

This command automatically enables disconnect supervision in the preconnect mode on the voice port if disconnect supervision is not already enabled with the **supervisory disconnect dualtone**command.

This command is applicable to analog FXO voice ports with loop-start signaling.

If false answering is detected, decrease the **sensitivity** setting. If answering detection is failing, increase the **sensitivity** setting.

Examples

The following example enables answer supervision on voice port 0/1/1:

```
voice-port 0/1/1
 supervisory answer dualtone
```

Related Commands

Command	Description
supervisory custom-cptone	Associates a class of custom call-progress tones with a voice port.

Command	Description
supervisory disconnect dualtone	Enables disconnect supervision on an FXO voice port.
timeouts ringing	Specifies the time that the calling voice port allows ringing to continue if a call is not answered.
voice class custom-cptone	Creates a voice class for defining custom call-progress tones.
voice class dualtone-detect-params	Modifies the frequency, power, and cadence tolerances of call-progress tones.

supervisory custom-cptone

To associate a class of custom call-progress tones with a voice port, use the **supervisory custom-cptone command in**voice-port configuration mode. To reset to the default, use the **no** form of this command.

supervisory custom-cptone *cptone-name*
no supervisory custom-cptone

Syntax Description

cptone -name	Descriptive identifier of the class of custom call-progress tones to be detected by a voice port. This name must match the *cptone-name* of a class of tones defined by the **voice class custom-cptone** command.

Command Default

U.S. standard call-progress tones are associated with a voice port.

Command Modes

Voice-port configuration (config-voiceport)

Command History

Release	Modification
12.1(5)XM	This command was introduced on the Cisco 2600 series, Cisco 3600 series, and Cisco MC3810.
12.2(2)T	This command was implemented on the Cisco 1750.

Usage Guidelines

This command associates a class of custom call-progress tones, defined by the **voice class custom-cptone** command, with a voice port.

You can associate the same custom call-progress tones to multiple voice ports.

You can associate only one class of custom call-progress tones with a voice port. If you associate a second class of custom call-progress tones with a voice port, the second class of custom tones replaces the one previously assigned.

This command is applicable to analog Foreign Exchange Office (FXO) voice ports with loop-start signaling.

Examples

The following example associates the class of custom call-progress tones named country-x with voice ports 1/4 and 1/5:

```
voice-port 1/4
 supervisory custom-cptone country-x
 exit
voice-port 1/5
 supervisory custom-cptone country-x
 exit
```

Related Commands

Command	Description
dualtone	Defines a call-progress tone to be detected.
supervisory answer dualtone	Enables answer supervision on an FXO voice port.

Command	Description
supervisory disconnect dualtone	Enables disconnect supervision on an FXO voice port.
voice class custom-cptone	Creates a voice class for defining custom call-progress tones.

supervisory disconnect

To enable a supervisory disconnect signal on Foreign Exchange Office (FXO) ports, use the **supervisory disconnect** command in voice-port configuration mode. To disable the signal, use the **no** form of this command.

supervisory disconnect
no supervisory disconnect

Syntax Description

This command has no arguments or keywords.

Command Default

Enabled

Command Modes

Voice-port configuration (config-voiceport)

Command History

Release	Modification
11.3(1)MA	This command was introduced on the Cisco MC3810.

Usage Guidelines

This command indicates whether supervisory disconnect signaling is available on the FXO port. Supervisory disconnect signaling is a power denial from the switch lasting at least 350 ms. When this condition is detected, the system interprets this as a disconnect indication from the switch and clears the call.

You should configure no supervisory disconnect on the voice port if there is no supervisory disconnect available from the switch.

Note If there is no disconnect supervision on the voice port, the interface could be left active if the caller abandons the call before the far end answers. After the router collects the dialed digits but before the called party answers, the router starts a tone detector. Within this time window, the tone detector listens for signals (such as a fast busy signal) that occur if the originating caller hangs up. If this occurs, the router interprets those tones as a disconnect indication and closes the window.

Examples

The following example configures supervisory disconnect on a voice port:

```
voice-port 2/1/0
 supervisory disconnect
```

supervisory disconnect anytone

To configure a Foreign Exchange Office (FXO) voice port to go on-hook if the router detects any tone from a PBX or the PSTN before an outgoing call is answered, use the **supervisory disconnect anytone command in**voice-port configuration mode. To disable the supervisory disconnect function, use the **no** form of this command.

supervisory disconnect anytone
no supervisory disconnect anytone

Syntax Description

This command has no arguments or keywords.

Command Default

The supervisory disconnect function is not enabled on voice ports.

Command Modes

Voice-port configuration (config-voiceport)

Command History

Release	Modification
12.1(5)XM	This command was introduced on the Cisco 2600 series, Cisco 3600 series, and Cisco MC3810.
12.2(2)T	This command was integrated into Cisco IOS Release 12.2(2)T and implemented on the Cisco 1750.

Usage Guidelines

Use this command to provide disconnect if the PBX or PSTN does not provide a supervisory tone. Examples of tones that trigger a disconnect include busy tone, fast busy tone, and dial tone.

This command is enabled only during call setup (before the call is answered).

You must enable echo cancellation; otherwise, ringback tone from the router can trigger a disconnect.

This command replaces the **no supervisory disconnect signal**command. If you enter thiscommand, the supervisory disconnect anytone feature is enabled, and the message supervisory disconnect anytoneis displayed when **show** commands are entered.

If you enter either the **supervisory disconnect anytone**command or the **no supervisory disconnect signal**command, answer supervision is automatically disabled.

Examples

The following example configures voice ports 1/4 and 1/5 to go on-hook if any tone from the PBX or PSTN is detected before the call is answered:

```
voice-port 1/4
 supervisory disconnect anytone
 exit
voice-port 1/5
 supervisory disconnect anytone
 exit
```

The following example disables the disconnect function on voice port 1/5:

```
voice-port 1/5
```

```
no supervisory disconnect anytone
exit
```

Related Commands

Command	Description
supervisory answer dualtone	Enables answer supervision on an FXO voice port.
supervisory disconnect dualtone	Enables disconnect supervision on an FXO voice port.
timeouts call-disconnect	Specifies the timeout value for releasing an FXO voice port when an incoming call is not answered.

supervisory disconnect dualtone

To enable disconnect supervision on a Foreign Exchange Office (FXO) voice port, use the **supervisory disconnect dualtone command in**voice-port configuration mode. To disable the supervisory disconnect function, use the **no** form of this command.

supervisory disconnect dualtone {**mid-call** | **pre-connect**}
no supervisory disconnect dualtone

Syntax Description

mid -call	Disconnect supervision operates throughout the duration of the call.
pre -connect	Disconnect supervision operates during call setup and stops when the called telephone goes off-hook.

Disconnect supervision is not enabled on voice ports.

Command Modes

Voice-port configuration (config-voiceport)

Command History

Release	Modification
12.1(5)XM	This command was introduced on the Cisco 2600 series, Cisco 3600 series, and Cisco MC3810.
12.2(2)T	This command was implemented on the Cisco 1750.

Usage Guidelines

This command configures an FXO voice port to disconnect calls when the router detects call-progress tones from a PBX or the PSTN. Disconnection occurs after the wait-release time specified on the voice port.

Disconnect supervision is automatically enabled in the preconnect mode on the voice port if the **supervisory answer dualtone**command is entered.

This feature is applicable to analog FXO voice ports with loop-start signaling.

Examples

The following example specifies tone detection during the entire call duration:

```
voice-port 1/5
 supervisory disconnect dualtone mid-call
 exit
```

The following example specifies tone detection only during call setup:

```
voice-port 0/1/1
 supervisory disconnect dualtone pre-connect
 exit
```

Related Commands

Command	Description
supervisory answer dualtone	Enables answer supervision on an FXO voice port.
supervisory custom-cptone	Associates a class of custom call-progress tones with a voice port.

Command	Description
timeouts call-disconnect	Specifies the timeout value for releasing an FXO voice port when an incoming call is not answered.
timeouts wait-release	Specifies the timeout value for releasing a voice port when an outgoing call is not answered.
voice class dualtone-detect-params	Modifies the frequency, power, and cadence tolerances of call-progress tones.

supervisory disconnect dualtone voice-class

To assign a previously configured voice class for Foreign Exchange Office (FXO) supervisory disconnect tone to a voice port, use the **supervisory disconnect dualtone voice-class** command in voice port configuration mode. To remove a voice class from a voice-port, use the **no** form of this command.

supervisory disconnect dualtone {**mid-call** | **pre-connect**} **voice-class** *tag*
no supervisory disconnect dualtone voice-class *tag*

Syntax Description

mid -call	Tone detection operates throughout the duration of a call.
pre -connect	Tone detection operates during call setup and stops when the called telephone goes off-hook.
tag	Unique identification number assigned to one voice class. The tag number maps to the tag number assigned using the **voice class dualtone** global configuration command. Range is from 1 to 10000.

Command Default

No voice class is assigned to a voice port.

Command Modes

Voice-port configuration (config-voiceport)

Command History

Release	Modification
12.1(3)T	This command was introduced on the Cisco 2600 series, Cisco 3600 series, and Cisco MC3810.

Usage Guidelines

You can apply an FXO supervisory disconnect tone voice class to multiple voice ports. You can assign only one FXO supervisory disconnect tone voice class to a voice port. If a second voice class is assigned to a voice port, the second voice class replaces the one previously assigned. You cannot assign separate FXO supervisory disconnect tone commands directly to the voice port.

This feature is applicable to analog FXO voice ports with loop-start signaling.

Examples

The following example assigns voice class 70 to FXO voice port 0/1/1 and specifies tone detection during the entire call duration:

```
voice-port 0/1/1
 no echo-cancel enable
 supervisory disconnect dualtone mid-call voice-class 70
```

The following example assigns voice class 80 to FXO voice port 0/1/1 and specifies tone detection only during call setup:

```
voice-port 0/1/1
 no echo-cancel enable
 supervisory disconnect dualtone pre-connect voice-class 80
```

Related Commands

Command	Description
channel-group	Defines the time slots of each T1 or E1 circuit.
mode	Sets the mode of the T1/E1 controller and enters specific configuration commands for each mode type in VoATM.
voice class dualtone	Creates a voice class for FXO tone detection parameters.

supervisory disconnect lcfo

To enable a supervisory disconnect signal on an FXS port, use the **supervisory disconnect lcfo** command in voice-port configuration mode. To disable the signal, use the **no** form of this command.

supervisory disconnect lcfo
no supervisory disconnect lcfo

Syntax Description

This command has no arguments or keywords.

Command Default

Enabled

Command Modes

Voice-port configuration (config-voiceport)

Command History

Release	Modification
12.1(5)YD	This command was introduced.
12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T.
12.4(2)T	Support was added for SCCP Telephony Control Application (STCAPP) analog voice ports.

Usage Guidelines

This command enables a disconnect indication by triggering a power denial using a loop current feed open (LCFO) signal on FXS ports with loop-start signaling. Third-party devices, such as an interactive voice response (IVR) system, can detect a disconnect and clear the call when it receives the power denial signal. To disable the power denial during the disconnect stage, use the **no supervisory disconnect lcfo** command. The duration of the power denial is set with the **timeouts power-denial** command.

Examples

The following example disables the power denial indication on voice port 2/0:

```
voice-port 2/0
 no supervisory disconnect lcfo
```

Related Commands

Command	Description
timeouts power-denial	Sets the duration of the power denial timeout for a specified FXS voice port.

supervisory dualtone-detect-params

To associate a class of modified tone-detection tolerance limits with a voice port, use the **supervisory dualtone-detect-params command in**voice-port configuration mode. To reset to the default, use the **no** form of this command.

supervisory dualtone-detect-params *tag*
no supervisory dualtone-detect-params

Syntax Description

tag	Tag number of the set of modified tone-detection tolerance limits to be associated with the voice port. The tag number must match the tag number of a voice class configured by the **voice class dualtone-detect-params**command. Range is from 1 to 10000.

Command Default

The default tone-detection tolerance limits are associated with voice ports.

Command Modes

Voice-port configuration (config-voiceport)

Command History

Release	Modification
12.1(5)XM	This command was introduced on the Cisco 2600 series, Cisco 3600 series, and Cisco MC3810.
12.2(2)T	This command was implemented on the Cisco 1750.

Usage Guidelines

This command associates a specific set of modified tone-detection tolerance limits, defined by the **voice class dualtone-detect-params**command, with a voice port.

You can associate the same class of modified tone-detection tolerance limits to multiple voice ports.

You can associate only one class of modified tone-detection tolerance limits to a voice port. If you associate a second class of modified tone-detection tolerance limits with a voice port, the second class replaces the one previously assigned.

This command is applicable to analog Foreign Exchange Office (FXO) voice ports with loop-start signaling.

Examples

The following example associates the class of modified tone-detection tolerance limits that has tag 70 with voice ports 1/5 and 1/6.

```
voice-port 1/5
 supervisory dualtone-detect-params 70
 exit
voice-port 1/6
 supervisory dualtone-detect-params 70
 exit
```

The following example restores the default tone-detection parameters to voice port 1/5.

```
voice-port 1/5
 no supervisory dualtone-detect-params
 exit
```

Related Commands

Command	Description
supervisory answer dualtone	Enables answer supervision on an FXO voice port.
supervisory disconnect dualtone	Enables disconnect supervision on an FXO voice port.
voice class dualtone-detect-params	Creates a voice class for call-progress tone-detection tolerance parameters.

supervisory sit us

To provide detection of eight standard U.S. special information tones (SITs) and certain nonstandard tones (including the AT&T SIT), and to report the detected tone with a preassigned disconnect cause code for disconnect supervision on a Foreign Exchange Office (FXO) voice port, use the **supervisory sit us**command in voice-port configuration mode. To turn off the detection and disconnect activity, use the **no** form of this command.

supervisory sit us [**all-tones**] [**tone-selector** *value*] [**immediate-release**]
no supervisory sit us

Syntax Description

all-tones	(Optional) Disconnects the call when a SIT or a nonstandard tone is detected.
tone-selector	(Optional) Defines a specific response for call-disconnect when a standard SIT or a nonstandard tone is detected on the incoming or outgoing call.
value	Acceptable values are 0, 1, 2, or 3: • 0--Detection of a standard SIT drops the call, but an AT&T SIT or a nonstandard tone does not cause a disconnect. • 1--Detection of either a standard SIT or nonstandard tone drops the call, but the AT&T SIT does not cause a disconnect. • 2--Detection of a standard SIT or an AT&T SIT results in a call disconnect, but any other nonstandard tone does not cause a disconnect. • 3--Detection of a standard SIT, AT&T SIT, or another nonstandard tone results in a disconnect.
immediate-release	(Optional) Disconnects the call immediately when a SIT is detected on the incoming or outgoing call. Nonstandard tones are ignored.

Command Default

No detection or disconnect occurs for the eight standard U.S. SITs, nonstandard tones, or the AT&T SIT on the FXO voice port for incoming and outgoing calls.

Command Modes

Voice-port configuration (config-voiceport)

Command History

Release	Modification
12.4(20)YA	This command was introduced.
12.4(22)T	This command was integrated into Cisco IOS Release 12.4(22)T.
12.4(24)T	The **all-tones** and **tone-selector**keywords and the *value* argument were added.

Usage Guidelines

This command configures an FXO voice port to detect and disconnect calls when the router detects call-progress tones from a PBX or the PSTN.

Prior to Cisco IOS Release 12.4(24)T, this command specifically detected eight standard U.S. SITs, but not nonstandard tones or the AT&T SIT. Beginning in Cisco IOS Release 12.4(24)T, the **tone-selector***value* option can be configured to detect nonstandard tones played by the service provider when the called number is invalid.

Disconnection occurs after the wait-release time specified on the voice port. Calls are disconnected immediately after a SIT is detected from the PSTN when the **immediate-release** keyword is configured. To configure the delay timeout before the system starts the process for releasing voice ports, use the **timeouts wait-release**command on the voice port.

The SIT reporting complies with standard Q.850 messages in order for fax servers to uniquely identify each condition. This capability is supported for analog FXO trunk and T1/E1 channel-associated signaling (CAS) FXO loop-start.



Note The SIT detection and reporting feature enabled by the **supervisory sit us** command is supported on c5510 and LSI digital signal processors (DSPs). No other DSPs support this feature.

The table below identifies eight standard U.S. SITs and their associated disconnect cause codes.



Note These eight tones are referred to as standard tones based on the tone frequencies and durations shown in the table. These tones are defined in the Telcordia Technologies specification GR-1162-CORE (which is specific to North America). There are other nonstandard SITs that can occur. The AT&T SIT is one of the more common examples of the other variations. The nonstandard SITs can have durations and frequencies comparable to the nominal values for the eight tone segments shown in the table below or the nonstandard SITs can deviate significantly from these nominal values. The **supervisory sit us** command has been modified in Cisco IOS Release 12.4(24)T to provide flexibility in handling these variations.

Table 235: Eight U.S. SITs and Associated Disconnect Cause Codes

Name	First Tone (Hz)	ms	Second Tone (Hz)	ms	Third Tone (Hz)	ms	Disconnect Cause Code
IC	913.8	274	1370.6	274	1776.7	380	8
VC	985.2	380	1370.6	274	1776.7	380	1
RO	985.2	274	1370.6	380	1776.7	380	86
RO	913.8	274	1428.5	380	1776.7	380	86
NC	913.8	380	1370.6	380	1776.7	380	34
NC	985.2	380	1428.5	380	1776.7	380	34
#1	913.8	380	1428.5	274	1776.7	274	21
#2	985.2	274	1428.5	274	1776.7	380	21

Examples

The following example shows how to enable SIT detection for the eight standard U.S. tones and provide for immediate disconnect on the voice port:

```
Router# configure terminal
Router(config)# voiceport 1/0/1
Router(config-voiceport)# supervisory sit us immediate-release
```

The following example shows how to enable SIT detection for all eight standard U.S. tones and configure the delay timeout for 10 seconds:

```
Router# configure terminal
Router(config)# voiceport 1/0/1
Router(config-voiceport)# supervisory sit us
Router(config-voiceport)# timeouts wait-release 10
```

The following example shows how to enable detection for a standard SIT or the AT&T SIT and to provide for immediate disconnect on the voice port (in this case, a nonstandard SIT does not cause a disconnect):

```
Router# configure terminal
Router(config)# voiceport 1/0/1
Router(config-voiceport)# supervisory sit us tone-selector 2 immediate-release
```

Related Commands

Command	Description
timeouts wait-release	Configures the delay timeout before the system starts the process for releasing voice ports.

supplementary-service h225-notify cid-update (dal peer)

To enable individual dial peers to send H.225 messages with caller-ID updates, use the **supplementary-service h225-notify cid-update** command in dal peer configuration mode. To disable the sending of H.225 messages with caller-ID updates, use the **no** form of this command.

supplementary-service h225-notify cid-update
no supplementary-service h225-notify cid-update

Syntax Description

This command has no arguments or keywords.

Command Default

H.225 messages with caller-ID updates are enabled.

Command Modes

dal peer configuration (config-dial-peer)

Command History

Release	Modification
12.3(7)T	This command was introduced.

Usage Guidelines

This command specifies that an individual dial peer should provide caller ID updates through H.225 notify messages when a call is transferred or forwarded between Cisco CallManager Express and Cisco CallManager systems. The default is that this behavior is enabled. The **no** form of the command disables caller-ID updates, which is not recommended. Use the **supplementary-service h225-notify cid-update** command in voice-service configuration mode to specify this capability globally.

If this command is enabled globally and enabled on a dial peer, the functionality is enabled for that dial peer. This is the default.

If this command is enabled globally and disabled on a dial peer, the functionality is disabled for that dial peer.

If this command is disabled globally and either enabled or disabled on a dial peer, the functionality is disabled for that dial peer.

Examples

The following example globally enables the sending of H.225 messages to transmit caller-ID updates and then disables that capability on dial peer 24.

```
Router(config)# voice service voip
Router(config-voi-serv)# supplementary-service h225-notify cid-update
Router(config-voi-serv)# exit
Router(config)# dial-peer voice 24 voip
Router(config-dial-peer)# no
 supplementary-service h225-notify cid-update
Router(config-dial-peer)# exit
```

Related Commands

Command	Description
dial-peer voice	Enters dial-peer configuration mode.

Command	Description
supplementary-service h225-notify cid-update (voice-service)	Globally enables the sending of H.225 messages with caller-ID updates.

supplementary-service h225-notify cid-update (voice-service)

To globally enable the sending of H.225 messages with caller-ID updates, use the **supplementary-service h225-notify cid-update** command in voice-service configuration mode. To disable the sending of H.225 messages with caller-ID updates, use the **no** form of this command.

supplementary-service h225-notify cid-update
no supplementary-service h225-notify cid-update

Syntax Description

This command has no arguments or keywords.

Command Default

H.225 messages with caller-ID updates are enabled.

Command Modes

Voice service configuration (config-voi-serv)

Command History

Release	Modification
12.3(7)T	This command was introduced.

Usage Guidelines

This command globally provides caller ID updates through H.225 notify messages when a call is transferred or forwarded between Cisco CallManager Express and Cisco CallManager systems. The default is that this behavior is enabled. The **no** form of the command disables caller-ID updates, which is not recommended. Use the **supplementary-service h225-notify cid-update** command in dial-peer configuration mode to specify this capability for individual dial peers.

If this command is enabled globally and enabled on a dial peer, the functionality is enabled for that dial peer. This is the default.

If this command is enabled globally and disabled on a dial peer, the functionality is disabled for that dial peer.

If this command is disabled globally and either enabled or disabled on a dial peer, the functionality is disabled for that dial peer.

Examples

The following example globally enables the sending of H.225 messages to transmit caller-ID updates and then disables that capability on dial peer 24.

```
Router(config)# voice service voip
Router(config-voi-serv)# supplementary-service h225-notify cid-update
Router(config-voi-serv)# exit
Router(config)# dial-peer voice 24 voip
Router(config-dial-peer)# no
 supplementary-service h225-notify cid-update
Router(config-dial-peer)# exit
```

Related Commands

Command	Description
supplementary-service h225-notify cid-update (dial-peer)	Enables the sending of H.225 messages with caller-ID updates for individual dial peers.

Command	Description
voice service voip	Enters voice-service configuration mode.

supplementary-service h450.2 (dial peer)

To enable H.450.2 supplementary services capabilities exchange for call transfers across a VoIP network for an individual dial peer, use the **supplementary-service h450.2** command in dial peer configuration mode. To disable H.450.2 capabilities for an individual dial peer, use the **no** form of this command.

supplementary-service h450.2
no supplementary-service h450.2

Syntax Description

This command has no arguments or keywords.

Command Default

H.450.2 supplementary services capabilities exchange is enabled.

Command Modes

Dial peer configuration (config-dial-peer)

Command History

Release	Modification
12.3(7)T	This command was introduced.

Usage Guidelines

This command specifies the use of the H.450.2 standard protocol for call transfers across a VoIP network for the calls handled by an individual dial peer. Use the **supplementary-service h450.2** command in voice-service configuration mode to specify H.450.2 capabilities at a global level.

If this command is enabled globally and enabled on a dial peer, the functionality is enabled for the dial peer. This is the default.

If this command is enabled globally and disabled on a dial peer, the functionality is disabled for the dial peer.

If this command is disabled globally and either enabled or disabled on a dial peer, the functionality is disabled for the dial peer.

Examples

The following example disables H.450.2 services for dial peer 37.

```
Router(config)# dial-peer voice 37 voip
Router(config-dial-peer)# destination-pattern 555....
Router(config-dial-peer)# session target ipv4:10.5.6.7

Router(config-dial-peer)# no supplementary-service h450.2

Router(config-dial-peer)# exit
```

Related Commands

Command	Description
dial-peer voice	Enters dial-peer configuration mode.
supplementary-service h450.2 (voice-service)	Globally enables H.450.2 capabilities for call transfers.

supplementary-service h450.2 (voice-service)

To globally enable H.450.2 supplementary services capabilities exchange for call transfers across a VoIP network, use the **supplementary-service h450.2**command in voice-service configuration mode. To disable H.450.2 capabilities globally, use the **no** form of this command.

supplementary-service h450.2
no supplementary-service h450.2

Syntax Description

This command has no arguments or keywords.

Command Default

H.450.2 supplementary services capabilities exchange is enabled.

Command Modes

Voice service configuration (config-voi-serv)

Command History

Release	Modification
12.3(7)T	This command was introduced.

Usage Guidelines

This command specifies global use of the H.450.2 standard protocol for call transfers for all calls across a VoIP network. Use the **no supplementary-service h450.2** command in dial-peer configuration mode to disable H.450.2 capabilities for individual dial peers.

If this command is enabled globally and enabled on a dial peer, the functionality is enabled for the dial peer. This is the default.

If this command is enabled globally and disabled on a dial peer, the functionality is disabled for the dial peer.

If this command is disabled globally and either enabled or disabled on a dial peer, the functionality is disabled for the dial peer.

Examples

The following example globally disables H.450.2 capabilities.

```
Router(config)# voice service voip
Router(config-voi-serv)# no supplementary-service h450.2

Router(config-voi-serv)# exit
```

Related Commands

Command	Description
supplementary-service h450.2 (dial-peer)	Enables H.450.2 call transfer capabilities for an individual dial peer.
voice-service voip	Enters voice-service configuration mode.

supplementary-service h450.3 (dial peer)

To enable H.450.3 supplementary services capabilities exchange for call forwarding across a VoIP network for an individual dial peer, use the **supplementary-service h450.3**command in dial peer configuration mode. To disable H.450.3 capabilities for an individual dial peer, use the **no** form of this command.

supplementary-service h450.3
no supplementary-service h450.3

Syntax Description

This command has no arguments or keywords.

Command Default

H.450.3 supplementary services capabilities exchange is enabled.

Command Modes

dial peer configuration (config-dial-peer)

Command History

Release	Modification
12.3(7)T	This command was introduced.

Usage Guidelines

This command specifies use of the H.450.3 standard protocol for call forwarding for calls handled by an individual dial peer. Use the **supplementary-service h450.3** command in voice-service configuration mode to specify H.450.3 capabilities at a global level.

If this command is enabled globally and enabled on a dial peer, the functionality is enabled for the dial peer. This is the default.

If this command is enabled globally and disabled on a dial peer, the functionality is disabled for the dial peer.

If this command is disabled globally and either enabled or disabled on a dial peer, the functionality is disabled for the dial peer.

Examples

The following example disables H.450.3 capabilities for dial peer 37.

```
Router(config)# dial-peer voice 37 voip
Router(config-dial-peer)# destination-pattern 555....
Router(config-dial-peer)# session target ipv4:10.5.6.7

Router(config-dial-peer)# no
 supplementary-service h450.3

Router(config-dial-peer)# exit
```

Related Commands

Command	Description
dial-peer voice	Enters dial-peer configuration mode.
supplementary-service h450.3 (voice-service)	Globally enables H.450.3 capabilities for call forwarding.

supplementary-service h450.3 (voice-service)

To globally enable H.450.3 supplementary services capabilities exchange for call forwarding across a VoIP network, use the **supplementary-service h450.3** command in voice-service configuration mode. To disable H.450.3 capabilities globally, use the **no** form of this command.

supplementary-service h450.3
no supplementary-service h450.3

Syntax Description

This command has no arguments or keywords.

Command Default

H.450.3 supplementary services capabilities exchange is enabled.

Command Modes

Voice service configuration (config-voi-serv)

Command History

Release	Modification
12.3(7)T	This command was introduced.

Usage Guidelines

This command specifies global use of the H.450.3 standard protocol for call forwarding across a VoIP network. Use the **no supplementary-service h450.3**command in dial-peer configuration mode to disable H.450.3 capabilities for individual dial peers.

If this command is enabled globally and enabled on a dial peer, the functionality is enabled for the dial peer. This is the default.

If this command is enabled globally and disabled on a dial peer, the functionality is disabled for the dial peer.

If this command is disabled globally and either enabled or disabled on a dial peer, the functionality is disabled for the dial peer.

Examples

The following example globally disables H.450.3 capabilities.

```
Router(config)# voice service voip
Router(config-voi-serv)# no supplementary-service h450.3

Router(config-voi-serv)# exit
```

Related Commands

Command	Description
supplementary-service h450.3 (dial-peer)	Enables H.450.3 call forwarding capabilities for an individual dial peer.
voice-service voip	Enters voice-service configuration mode.

supplementary-service h450.7

To globally enable H.450.7 supplementary services capabilities exchange for message-waiting indication (MWI) across a VoIP network, use the **supplementary-service h450.7** command in voice-service or dial-peer configuration mode. To return to the default, use the **no** form of this command.

supplementary-service h450.7
no supplementary-service h450.7

Syntax Description

There are no keywords or arguments.

Command Default

H.450.7 supplementary services are disabled.

Command Modes

Voice service configuration (config-voi-serv)
Dial-peer configuration (config-dial-peer)

Command History

Cisco IOS Release	Modification
12.4(4)XC	This command was introduced.
12.4(9)T	This command was integrated into Cisco IOS Release 12.4(9)T.

Usage Guidelines

Use this command when you are implementing QSIG supplementary service features that use the H.450.7 standard.

Use this command in voice-service configuration mode to affect all dial peers globally. Use this command in dial-peer configuration mode to affect an individual dial peer:

If the **supplementary-service h450.7** command is not in use, the services are globally disabled by default.

If the **supplementary-service h450.7** command is not in use in voice-service configuration mode, you can use this command in dial-peer configuration mode to enable the services on individual dial peers.

If the **supplementary-service h450.7** command is in use in voice-service configuration mode, the services are globally enabled and you cannot disable the services on individual dial peers.

Examples

The following example shows how to globally enable H.450.7 supplemental services:

```
voice service voip
 supplementary-service h450.7
```

The following example shows how to enable H.450.7 supplemental services on dial peer 256:

```
dial-peer voice 256 voip
 supplementary-service h450.7
```

Related Commands

Command	Description
dial-peer voice	Enters dial-peer configuration mode.

Command	Description
voice service voip	Enters voice-service configuration mode.

supplementary-service h450.12 (dial peer)

To enable H.450.12 supplementary services capabilities exchange for call transfers across a VoIP network for an individual dial peer, use the **supplementary-service h450.12** command in dial peer configuration mode. To disable H.450.12 capabilities for an individual dial peer, use the **no** form of this command.

supplementary-service h450.12
no supplementary-service h450.12

Syntax Description

This command has no arguments or keywords.

Command Default

H.450.12 supplementary services capabilities exchange is disabled.

Command Modes

Dial peer configuration (config-dial-peer)

Command History

Release	Modification
12.3(7)T	This command was introduced.

Usage Guidelines

This command specifies use of the H.450.12 standard protocol for call transfers across a VoIP network for calls handled by an individual dial peer. Use the **supplementary-service h450.12** command in voice-service configuration mode to specify H.450.12 capabilities at a global level.

If this command is enabled globally and enabled on a dial peer, the functionality is enabled for the dial peer.

If this command is enabled globally and disabled on a dial peer, the functionality is enabled for the dial peer.

If this command is disabled globally and enabled on a dial peer, the functionality is enabled for the dial peer.

If this command is disabled globally and disabled on a dial peer, the functionality is disabled for the dial peer. This is the default.

Examples

The following example enables H.450.12 capabilities on dial peer 37.

```
Router(config)# dial-peer voice 37 voip
Router(config-dial-peer)# destination-pattern 555....
Router(config-dial-peer)# session target ipv4:10.5.6.7

Router(config-dial-peer)# supplementary-service h450.12

Router(config-dial-peer)# exit
```

Related Commands

Command	Description
dial-peer voice	Enters dial-peer configuration mode.
supplementary-service h450.12 (voice-service)	Globally enables H.450.12 capabilities.

supplementary-service h450.12 (voice-service)

To globally enable H.450.12 supplementary services capabilities exchange for call transfers across a VoIP network, use the **supplementary-service h450.12**command in voice-service configuration mode. To disable H.450.12 capabilities globally, use the **no** form of this command.

supplementary-service h450.12 [**advertise-only**]
no supplementary-service h450.12 [**advertise-only**]

Syntax Description

advertise-only	(Optional) Advertises H.450 capabilities to the remote end but does not require H.450.12 responses.

Command Default

H.450.12 supplementary services capabilities exchange is disabled.

Command Modes

Voice service configuration (config-voi-serv)

Command History

Release	Modification
12.3(7)T	This command was introduced.

Usage Guidelines

The H.450.12 standard provides a means to advertise and discover H.450.2 call transfer and H.450.3 call forwarding capabilities in voice gateway endpoints on a call-by-call basis. When H.450.12 is enabled, use of H.450.2 and H.450.3 standards is disabled for call transfers and call forwards unless a positive H.450.12 indication is received from all the other VoIP endpoints involved in the call. If positive H.450.12 indications are received, the router uses the H.450.2 standard for call transfers and the H.450.3 standard for call forwarding. If a positive H.450.12 indication is not received, the router uses the alternative method that you have configured for call transfers and forwards, which, for Cisco CallManager Express (Cisco CME) 3.1 systems, may be either hairpin call routing or an H.450 tandem gateway. This command is useful when you have a mixed network with some endpoints that support H.450.2 and H.450.3 standards and other endpoints that do not support those standards.

This command specifies the global use of the H.450.12 standard protocol for all calls across a VoIP network. Use the **supplementary-service h450.12** command in dial-peer configuration mode to specify H.450.12 capabilities for individual dial peers.

If this command is enabled globally and enabled on a dial peer, the functionality is enabled for the dial peer.

If this command is enabled globally and disabled on a dial peer, the functionality is enabled for the dial peer.

If this command is disabled globally and enabled on a dial peer, the functionality is enabled for the dial peer.

If this command is disabled globally and disabled on a dial peer, the functionality is disabled for the dial peer. This is the default.

Use the **advertise-only** keyword on a Cisco CME 3.1 system when you have only Cisco CME 3.0 systems in your network in addition to Cisco CME 3.1 systems. Cisco CME 3.0 systems can use H.450.2 and H.450.3 standards, but are unable to respond to H.450.12 queries. The **advertise-only** keyword enables a Cisco CME 3.1 system to bypass the requirement that a system respond to an H.450.12 query in order to use H.450.2 and H.450.3 standards for transferring and forwarding calls.

Examples

The following example enables H.450.12 capabilities at a global level.

```
Router(config)# voice service voip
Router(config-voi-serv)# supplementary-service h450.12

Router(config-voi-serv)# exit
```

The following example enables H.450.12 capabilities at a global level in advertise-only mode on a Cisco CME 3.1 system to enable call transfers using the H.450.2 standard and call forwards using the H.450.3 standard with Cisco CME 3.0 systems in the network.

```
Router(config)# voice service voip
Router(config-voi-serv)# supplementary-service h450.12
 advertise-only
Router(config-voi-serv)# exit
```

Related Commands

Command	Description
supplementary-service h450.12 (dial-peer)	Enables H.450.12 capabilities for an individual dial peer.
voice-service voip	Enters voice-service configuration mode.

supplementary-service media-renegotiate

To globally enable midcall media renegotiation for supplementary services, use the **supplementary-service media-renegotiate** command in voice-service configuration mode. To disable midcall media renegotiation for supplementary services, use the **no** form of this command.

supplementary-service media-renegotiate
no supplementary-service media-renegotiate

Syntax Description

This command has no arguments or keywords.

Command Default

Midcall media renegotiation for supplementary services is disabled.

Command Modes

Voice-service configuration (config-voi-serv)

Command History

Release	Modification
12.4(11)XW1	This command was introduced.
12.4(20)T	This command was integrated into Cisco IOS Release 12.4(20)T.
Cisco IOS XE Cupertino 17.7.1a	Introduced support for YANG models.

Usage Guidelines

This command enables midcall media renegotiation, or key renegotiation, for all calls across a VoIP network. To implement media encryption, the two endpoints controlled by Cisco Unified Communications Manager Express (Cisco Unified CME) need to exchange keys that they will use to encrypt and decrypt packets. Midcall key renegotiation is required to support interoperation and supplementary services among multiple VoIP suites in a secure media environment using Secure Real-Time Transport Protocol (SRTP).

Note The video part of a video stream will not play if the **supplementary-service media-renegotiate** command is configured in voice-service configuration mode.

Examples

The following example enables midcall media renegotiation for supplementary services at a global level.

```
Router(config)# voice service voip
Router(config-voi-serv)# supplementary-service media-renegotiate
Router(config-voi-serv)# exit
```

supplementary-service qsig call-forward

To specify that calls are using QSIG and require supplementary services for call forwarding, use the **supplementary-service qsig call-forward**command in voice-service or dial-peer configuration mode. To return to the default, use the **no** form of this command.

supplementary-service qsig call-forward
no supplementary-service qsig call-forward

Syntax Description

This command has no keywords or arguments.

Command Default

The functionality is disabled.

Command Modes

Voice service configuration (config-voi-serv)
Dial-peer configuration (dial-peer-config)

Command History

Cisco IOS Release	Modification
12.4(4)XC	This command was introduced.
12.4(9)T	This command was integrated into Cisco IOS Release 12.4(9)T.

Usage Guidelines

This command provides QSIG call-forwarding supplementary services (ISO 13873) when necessary to forward calls to another number.

Use this command in voice-service configuration mode, which is enabled by the **voice service pots**command, to affect all POTS dial peers globally. Use this command in dial-peer configuration mode, which is enabled by the **dial-peer voice** command, to affect a single POTS dial peer.

If you are not using the **supplementary-service qsig call-forward**command, the services are globally disabled by default.

If you are not using the **supplementary-service qsig call-forward** command in voice-service configuration mode, you can use this command in dial-peer configuration mode to enable the services on individual POTS dial peers.

If you are using the **supplementary-service qsig call-forward** command in voice-service configuration mode, this feature is globally enabled and you cannot disable the services on individual POTS dial peers.

Examples

The following example shows how to enable QSIG call-forwarding treatment for all POTS calls:

```
Router(config)# voice service pots
Router(conf-voi-serv)# supplementary-service qsig call-forward
```

The following example shows how to enable QSIG call-forwarding treatment for calls on POTS dial-peer 23:

```
Router(config)# dial-peer voice 23 pots
Router(config-dial-peer)# supplementary-service qsig call-forward
```

Related Commands

Command	Description
dial-peer voice	Enters dial-peer configuration mode.
voice service voip	Enters voice-service configuration mode.

supplementary-service sip

To enable SIP supplementary service capabilities for call forwarding and call transfers across a SIP network, use the **supplementary-service sip** command in dial peer voice or voice service VOIP configuration mode. To disable supplementary service capabilities, use the **no** form of this command.

supplementary-service sip {**handle-replaces** | **moved-temporarily** | **refer**}
no supplementary-service sip {**handle-replaces** | **moved-temporarily** | **refer**}

Syntax Description

handle-replaces	Replaces the Dialog-ID in the Replaces Header with the peer Dialog-ID.
moved-temporarily	Enables SIP Redirect response for call forwarding.
refer	Enables SIP REFER message for call transfers.

Command Default

SIP supplementary service capabilities are enabled globally.

Command Modes

Dial peer voice configuration (config-dial-peer)

Voice service configuration (conf-voi-serv)

Command History

Release	Modification
12.4(11)XJ	This command was introduced.
12.4(15)T	This command was integrated into Cisco IOS Release 12.4(15)T.
15.2(2)T1	This command was modified. The **handle-replaces** keyword was introduced.
15.3(1)T	This command was modified. With CSCub47586, if an INVITE (incoming call or incoming forward) with a diversion header is received while the **no supplementary-service sip moved-temporarily** form of this command is enabled, on either an inbound call leg or an outbound call leg, the call is disconnected.
Cisco IOS XE Amsterdam 17.2.1r	Introduced support for YANG models.

Usage Guidelines

The **supplementary-service sip refer** command enables REFER message pass-through on a router.

The **no** form of the **supplementary-service sip** command allows you to disable a supplementary service feature (call forwarding or call transfer) if the destination gateway does not support the supplementary service. You can disable the feature either globally or for a specific SIP trunk (dial peer).

- The **no supplementary-service sip handle-replaces** command replaces the Dialog-ID in the Replaces Header with the peer Dialog-ID.
- The **no supplementary-service sip moved-temporarily** command prevents the router from sending a redirect response to the destination for call forwarding. SDP Passthrough is not supported in 302-consumption mode or Refer-consumption mode. With CSCub47586, if an INVITE (incoming call

or incoming forward) with a diversion header is received while SDP Pass through is enabled on either an inbound call leg or an outbound call leg, the call is disconnected.

- The **no supplementary-service sip refer** command prevents the router from forwarding a REFER message to the destination for call transfers. The router instead attempts to initiate a hairpin call to the new target.

If this command is enabled globally and disabled on a dial peer, the functionality is disabled for the dial peer.

If this command is disabled globally and either enabled or disabled on a dial peer, the functionality is disabled for the dial peer.

On Cisco Unified Communications Manager Express (CME), this command is supported for calls between SIP phones and for calls between SCCP phones. It is not supported for a mixture of SCCP and SIP phones; for example, it has no effect for calls from an SCCP phone to a SIP phone. On the Cisco UBE, this command is supported for SIP trunk-to-SIP trunk calls.

Examples

The following example shows how to disable SIP call transfer capabilities for dial peer 37:

```
Device(config)# dial-peer voice 37 voip
Device(config-dial-peer)# destination-pattern 555....
Device(config-dial-peer)# session target ipv4:10.5.6.7

Device(config-dial-peer)# no supplementary-service sip refer
```

The following example shows how to disable SIP call forwarding capabilities globally:

```
Device(config)# voice service voip
Device(conf-voi-serv)# no supplementary-service sip moved-temporarily
```

The following example shows how to enable a REFER message pass-through on the Cisco UBE globally and how to disable the Refer-To header modification:

```
Device(config)# voice service voip
Device(conf-voi-serv)# supplementary-service sip refer
Device(conf-voi-serv)# sip
Device(conf-serv-sip)# referto-passing
```

The following example shows how to enable a REFER message consumption on the Cisco UBE globally:

```
Device(config)# voice service voip
Device(conf-voi-serv)# no supplementary-service sip refer
```

The following example shows how to enable REFER message consumption on the Cisco UBE for dial peer 22:

```
Device(config)# dial-peer voice 22 voip
Device(config-dial-peer)# no supplementary-service sip refer
```

The following example shows how to enable a REFER message to replace the Dialog-ID in the Replaces Header with the peer Dialog-ID on the Cisco UBE for dial peer:

```
Device(config)# dial-peer voice 34 voip
Device(config-dial-peer)# no supplementary-service sip handle-replaces [system]
```

The following example shows how to enable a REFER message to replace the Dialog-ID in the Replaces Header with the peer Dialog-ID on the Cisco UBE globally:

```
Device(config)# voice service voip
Device(conf-voi-serv)# no supplementary-service sip handle-replaces
```

Related Commands

Command	Description
supplementary-service h450.2 (voice-service)	Globally enables H.450.2 capabilities for call transfer.
supplementary-service h450.3 (voice-service)	Globally enables H.450.3 capabilities for call forwarding.
referto-passing	Disables dial peer lookup and modification of the Refer-To header while passing across REFER message on the Cisco UBE during a call transfer.

supported language

To configure Session Initiation Protocol (SIP) Accept-Language header support, use the **supported-language**command in voice service or dial-peer voice configuration mode. To disable Accept-Language header support, use the **no** form of this command.

supported-language *language-code* **language-param** *qvalue*
no supported-language *language-code*

Syntax Description

language -code	Any of 139 languages designated by a two-letter ISO-639 country code.
qvalue	The priority of the language, with languages sorted in descending order according the assigned parameter value. Valid values include zero, one, or a decimal fraction in the range .001 through .999. Default is 1, the highest priority.
language -param	Specifies language preferences by associating a parameter with the language being configured.

Command Default

qvalue: 1

Command Modes

Dial-peer voice configuration (config-dial-peer)
Voice service configuration (config-voi-serv)

Command History

Release	Modification
12.3(1)	This command was introduced.

Usage Guidelines

To include the Accept-Language header in outgoing SIP INVITE messages, and enable Accept-Language header support on specific trunk groups with different language requirements, use dial-peer voice configuration mode, which is enabled by the dial-peer voice command . To enable Accept-Language headers to be included in both SIP INVITE messages and OPTIONS responses, use voice service configuration mode, enabled by the voice service pots command. If both voice service and dial-peer voice mode accept-language support are configured, and there are no dial-peer matches, the outgoing INVITE message contains the voice service specified languages. Otherwise, the INVITE contains the dial-peer configured languages.

The SIP Accept-Language Header Support feature supports 139 languages which are designated by a two-letter ISO-639 country code. The following is a partial list of supported language codes and languages. To display a complete listing use the help command supported-language ?.

- • **AR** --Arabic
  • **ZH** --Chinese
  • EN--English
  • EO--Esperanto
  • DE--German
  • EL--Greek
  • HE--Hebrew
  • GA--Irish
  • IT--Italian

- JA--Japanese
- KO--Korean
- RU--Russian
- ES--Spanish
- SW--Swahili
- SV--Swedish
- VI--Vietnamese
- YI--Yiddish
- ZU--Zulu

Examples

The following example configures Italian to be the preferred language, followed by Greek:

```
s
upported-language IT language-param .9
supported-language EL language-param .8
```

Related Commands

Command	Description
show dial-peer voice	Displays the configuration for all VoIP and POTS dial peers.

suppress

To suppress accounting for a specific call leg, use the **suppress** command in gateway accounting AAA configuration mode. To reenable accounting for that leg, use the **no** form of this command.

suppress [**pots** | **rotary** | **voip**]
no suppress [**pots** | **rotary** | **voip**]

Syntax Description

pots	(Optional) POTS call leg.
rotary	(Optional) Rotary dial peer.
voip	(Optional) VoIP call leg.

Command Default

Accounting is enabled.

Command Modes

Gateway accounting AAA configuration (config-gw-accounting-aaa)

Command History

Release	Modification
12.2(11)T	This command was introduced.

Usage Guidelines

Use this command to turn off accounting for a specific call leg.

If both incoming and outgoing call legs are of the same type, no accounting packets are generated.

Use the **rotary** keyword to suppress excess start and stop accounting records. This causes only one pair of records to be generated for every connection attempt through a dial peer.

Examples

The following example suppresses accounting for the POTS call leg.

```
suppress pots
```

Related Commands

Command	Description
debug suppress rotary	Displays connection attempt statistics.
gw-accounting aaa	Enables VoIP gateway accounting.

survivability single-register

To enable survivability for phones that register with Nano CUBE using single register request, execute **survivability single-register** command in voice service voip >> sip configuration mode. To disable, use **no** form of this command.

survivability single-register
no survivability single-register

Syntax Description

This command has no arguments or keywords.

Command Default

Survivability is not enabled for phones that send single register request.

Command Modes

voice service voip >> sip

Command History

Release	Modification
Cisco IOS 15.6(1)T	This command was introduced.

Usage Guidelines

When this command is configured, Nano CUBE always checks for the response from remote side. Request timeout on WAN side or response other than 200, 4XX, and 3XX received by Nano CUBE from SBC enables the survivability.

Example

```
Device> enable
Device# configure terminal
Device(config)#  voice service voip
Device(conf-voi-serv)# sip
Device(conf-serv-sip)# survivability single-register
```

suspend-resume (SIP)

To enable SIP Suspend and Resume functionality, use the **suspend-resume** command in SIP user agent configuration mode. To disable SIP Suspend and Resume functionality, use the **no** form of this command.

suspend-resume
no suspend-resume

Syntax Description

This command has no arguments or keywords.

Command Default

Enabled

Command Modes

SIP UA configuration (config-sip-ua)

Command History

Release	Modification
12.2(15)T	This command was introduced.

Usage Guidelines

Session Initiation Protocol (SIP) gateways are now enabled to use Suspend and Resume. Suspend and Resume are basic functions of ISDN and ISDN User Part (ISUP) signaling procedures. A Suspend message temporarily halts communication (call hold), and a Resume message is received after a Suspend message and continues the communication.

Examples

The following example disables Suspend and Resume functionality:

```
Router(config)# sip-ua
Router(config-sip-ua)# no suspend-resume
```

Related Commands

Command	Description
show sip -ua status	Displays SIP UA status.
sip -ua	Enables the SIP user-agent configuration commands.

switchback interval

To set the amount of time that the digital signal processor (DSP) farm waits before polling the primary Cisco Unified CallManager when the current Cisco Unified CallManager switchback connection fails, use the **switchback interval**command in SCCP Cisco Unified CallManager configuration mode. To reset the amount of time to the default value, use the **no** form of this command.

switchback interval *seconds*
no switchback interval

Syntax Description

seconds	Timer value, in seconds. Range is 1 to 3600. Default is 60.

Command Default

60 seconds

Command Modes

SCCP Cisco Unified CallManager configuration (config-sccp-ccm)

Command History

Release	Modification
12.3(8)T	This command was introduced.

Usage Guidelines

The optimum setting for this command depends on the platform and your individual network characteristics. Adjust the switchback interval value to meet your needs.

Examples

The following example sets the length of time the DSP farm waits to before polling the primary Cisco Unified CallManager to 120 seconds (2 minutes):

```
Router(conf-sccp-ccm)# switchback interval 120
```

Related Commands

Command	Description
connect interval	Specifies how many times a given profile attempts to connect to the specific CiscoUnified CallManager.
sccp ccm group	Creates a Cisco CallManger group and enters SCCP Cisco CallManager configuration mode.
switchback method	Sets the method that Cisco Unified CallManager uses to initiate the switchback process.
switchover method	Sets the switchover method that the SCCP client uses when the communication between the active Cisco Unified CallManager and the SCCP client goes down.

switchback method

To set the Cisco Unified CallManager switchback method, use the **switchback method**command in Skinny SCCP Cisco Unified CallManager configuration mode. To reset to the default value, use the **no** form of this command.

switchback method {**graceful** | **guard** [*timeout-guard-value*] | **immediate** | **uptime** *uptime-timeout-value*}
no switchback method

Syntax Description

graceful	Selects the graceful switchback method.
guard	Selects the graceful with guard switchback method.
guard timeout value	(Optional) Timeout value, in seconds. Range is from 60 to 172800. Default is 7200.
immediate	Selects the immediate switchback method.
uptime	Selects the uptime-delay switchback method.
uptime timeout value	(Optional) Timeout value, in seconds. Range is from 60 to 172800. Default is 7200.

Command Default

Guard is the default switchback method, with a timeout value of 7200 seconds.

Command Modes

SCCP Cisco Unified CallManager configuration (config-sccp-ccm)

Command History

Release	Modification
12.3(8)T	This command was introduced.

Usage Guidelines

Use this command to set the Cisco Unified CallManager switchback method. When a switch-over happens with the secondary Cisco Unified CallManager initiates the switchback process with that higher-order Cisco Unified CallManager. The available switchback methods follow:

- graceful--The Cisco Unified CallManager switchback happens only after all the active sessions are terminated gracefully.
- guard--The Cisco Unified CallManager switchback happens either when the active sessions are terminated gracefully or when the guard timer expires, whichever happens first.
- immediate--Performs the Cisco Unified CallManager switchback to the higher order CiscoUnified CallManager immediately as soon as the timer expires, whether there is an active connection or not.
- uptime--Once the higher-order Cisco Unified CallManager comes alive, the uptime timer in initiated.

Note The optimum setting for this command depends on the platform and your individual network characteristics. Adjust the switchback method to meet your needs.

Examples

The following example sets the Cisco Unified CallManager switchback method to happen only after all the active sessions are terminated gracefully.

```
Router(config-sccp-ccm)# switchback method graceful
```

Related Commands

Command	Description
connect interval	Specifies the amount of time that a DSP farm profile waits before attempting to connect to a Cisco Unified CallManager when the current Cisco Unified CallManager fails to connect.
sccp ccm group	Creates a Cisco CallManger group and enters SCCP Cisco CallManager configuration mode.
switchback interval	Sets the amount of time that the DSP farm waits before polling the primary Cisco Unified CallManager when the current Cisco Unified CallManager fails to connect.
switchover method	Sets the switchover method that the SCCP client uses when the communication between the active Cisco Unified CallManager and the SCCP client goes down.

switchover method

To set the switchover method that the Skinny Client Control Protocol (SCCP) client uses when the communication link between the active Cisco Unified CallManager and the SCCP client goes down, use the switchover methodcommand in SCCP Cisco Unified CallManager configuration mode. To reset the switchover method to the default, use the **no** form of this command.

switchover method {**graceful** | **immediate**}
no switchover method

Syntax Description

graceful	Switchover happens only after all the active sessions are terminated gracefully.
immediate	Switches over to any one of the secondary Cisco Unified CallManager immediately.

Command Default

Graceful

Command Modes

SCCP Cisco Unified CallManager configuration (config-sccp-ccm)

Command History

Release	Modification
12.3(8)T	This command was introduced.

Usage Guidelines

When the communication link between the active Cisco Unified CallManager and the SCCP client goes down the SCCP client tries to connect to one of the secondary Cisco Unified CallManagers using one of the following switchover methods:

- graceful--The Cisco Unified CallManager switchover happens only after all the active sessions are terminated gracefully.
- immediate--Regardless of whether there is an active connection or not the SCCP client switches over to one of the secondary Cisco Unified CallManagers immediately. If the SCCP Client is not able to connect to a secondary Cisco CUnified allManager, it continues polling for a CiscoUnified CallManager connection.

Note The optimum setting for this command depends on the platform and your individual network characteristics. Adjust the switchover method to meet your needs.

Examples

The following example sets the switchover method that the SCCP client uses to connect to a secondary Cisco Unified CallManager to happen only after all the active sessions are terminated gracefully:

```
Router (config-sccp-ccm)# switchover method graceful
```

Related Commands

Command	Description
connect interval	Specifies the amount of time that a DSP farm profile waits before attempting to connect to a Cisco Unified CallManager when the current Cisco Unified CallManager fails to connect.
sccp ccm group	Creates a Cisco CallManger group and enters the SCCP Cisco CallManager configuration mode.
switchback interval	Sets the amount of time that the DSP farm waits before polling the primary Cisco Unified CallManager when the current Cisco Unified CallManager fails to connect.
switchback method	Sets the method that Cisco Unified CallManager uses to initiate the switchback process.