

O through R

- outbound data-pid, on page 4
- outbound data-rate, on page 5
- outbound frequency, on page 6
- outbound id, on page 7
- outbound modulation-type, on page 8
- outbound sync ip address, on page 9
- outbound viterbi-rate, on page 10
- output, on page 11
- overhead c2, on page 13
- overhead j0, on page 14
- overhead j1, on page 16
- overhead tunnel, on page 18
- overhead s1s0, on page 20
- password (satellite initial configuration), on page 21
- payload-compression, on page 22
- payload-size dejitter-buffer, on page 23
- payload-size, on page 25
- physical-interface, on page 30
- physical-layer, on page 31
- platform console, on page 33
- platform cwan acl software-switched, on page 34
- platform enable controller mediaType , on page 35
- platform hardware throughput crypto, on page 36
- platform hardware throughput level, on page 39
- platform ip features sequential, on page 42
- platform punt-keepalive, on page 44
- platform punt-arp-unicast cpu-queue-host, on page 46
- platform scp retry interval, on page 47
- platform smart-sfp, on page 48
- platform time-source, on page 50
- platform trace boottime process forwarding-manager module interfaces, on page 52
- pm fec threshold, on page 54
- pm optics report, on page 55

- pm otn report, on page 56
- pm optics threshold, on page 59
- pm otn threshold, on page 60
- port (interface), on page 61
- port access-map, on page 62
- port-channel hash-distribution, on page 64
- port-channel load-balance, on page 65
- port-channel load-balance (interface), on page 68
- port-channel load-balance mpls, on page 70
- port-channel load-balance weighted rebalance, on page 72
- port-channel load-balancing vlan-manual, on page 73
- port-channel load-defer, on page 75
- port-channel min-links, on page 77
- port-channel per-module load-balance, on page 78
- port-channel port load-defer, on page 79
- port-channel standalone-disable, on page 81
- pos ais-shut, on page 82
- pos delay triggers, on page 83
- pos flag, on page 86
- pos flag s1-byte rx-communicate, on page 88
- pos flag s1-byte tx, on page 89
- pos framing, on page 90
- pos report, on page 91
- pos scramble-atm, on page 93
- pos threshold, on page 95
- power inline, on page 97
- power enable, on page 102
- power inline, on page 103
- power redundancy-mode, on page 108
- ppp link, on page 109
- ppp loopback no-backoff, on page 111
- ppp multilink mrru, on page 113
- pri-group, on page 117
- priority1, on page 118
- priority2, on page 119
- proactive enable, on page 120
- proactive rvrt-threshold, on page 121
- proactive rvrt-window, on page 122
- proactive trig-threshold , on page 123
- protection-group, on page 125
- protection-group [working | protect], on page 126
- protocol gre, on page 127
- ptp clock, on page 128
- pulse-time, on page 129
- rate, on page 131
- recovered-clock, on page 133

- redundancy, on page 134
- redundancy all-active replicate, on page 139
- redundancy force-switchover, on page 140
- redundancy handover, on page 143
- redundancy stateful, on page 145
- remote command, on page 146
- remote-span, on page 148
- remote login, on page 149
- reset (alarm-interface), on page 151
- retry, on page 152
- ring-speed, on page 153
- rj45-auto-detect-polarity, on page 154

outbound data-pid



Note Effective with Cisco IOS Release 12.4(2)T, this command is superseded by the **outboundpidmanagement** command. The **outbounddata-pid** command is still available, but use of the **outboundpidmanagement** command is recommended.

To specify the outbound data packet identification (PID) number, use the **outbounddata-pid** command in satellite initial configuration mode. To remove the PID number configuration, use the **no** form of this command.

outbound data-pid *number*
no outbound data-pid

Syntax Description

number	Packet identification (PID) number in the range from 1 to 8190.

Command Default

No default behavior or values

Command Modes

Satellite initial configuration

Command History

Release	Modification
12.3(14)T	This command was introduced.
12.4(2)T	This command was superseded by the**outboundpidmanagement** command.

Usage Guidelines

This command is typically used by an installation technician. Do not use this command unless your satellite service provider instructs you to perform the satellite initial configuration and provides all necessary parameter values.

Examples

The following example shows how to specify the outbound data PID number:

```
Router(sat-init-config)# outbound data-pid 3000
```

outbound data-rate

To specify the VSAT data rate, use the **outbounddata-rate** command in satellite initial configuration mode. To remove the data rate configuration, use the **no** form of this command.

outbound data-rate *rate*
no outbound data-rate

Syntax Description

rate	VSAT data rate in the range from 250000 to 73000000 bits per second.

Command Default

No default behavior or values

Command Modes

Satellite initial configuration

Command History

Release	Modification
12.3(14)T	This command was introduced.

Usage Guidelines

This command is typically used by an installation technician. Do not use this command unless your satellite service provider instructs you to perform the satellite initial configuration and provides all necessary parameter values.

Examples

The following example shows how to specify the VSAT data rate:

```
Router(sat-init-config)# outbound data-rate 450000
```

outbound frequency

To specify the VSAT outbound frequency, use the **outboundfrequency** command in satellite initial configuration mode. To remove the outbound frequency configuration, use the **no** form of this command.

outbound frequency *frequency*
no outbound frequency

Syntax Description

frequency	VSAT outbound frequency in the range from 950000 to 2150000 kilohertz.

Command Default

No default behavior or values

Command Modes

Satellite initial configuration

Command History

Release	Modification
12.3(14)T	This command was introduced.

Usage Guidelines

This command is typically used by an installation technician. Do not use this command unless your satellite service provider instructs you to perform the satellite initial configuration and provides all necessary parameter values.

Examples

The following example shows how to configure the VSAT outbound frequency:

```
Router(sat-init-config)# outbound frequency 950000
```

outbound id

To specify the VSAT outbound ID, use the **outboundid**command in satellite initial configuration mode. To remove the outbound ID configuration, use the **no** form of this command.

outbound id *number*
no outbound id

Syntax Description

number	ID number in the range from 0 to 255.

Command Default

No default behavior or values

Command Modes

Satellite initial configuration

Command History

Release	Modification
12.3(14)T	This command was introduced.

Usage Guidelines

This command is typically used by an installation technician. Do not use this command unless your satellite service provider instructs you to perform the satellite initial configuration and provides all necessary parameter values.

Examples

The following example shows how to configure the VSAT outbound ID:

```
Router(sat-init-config)# outbound id 95
```

outbound modulation-type

To specify the VSAT modulation type, use the **outboundmodulation-type** command in satellite initial configuration mode. To remove the VSAT modulation type configuration, use the **no** form of this command.

outbound modulation-type {**DVB** | **TURBO_QPSK** | **8PSK**}
no outbound modulation-type

Syntax Description

DVB	Digital Video Broadcasting for satellite.
TURBO_QPSK	Turbo-coded quadrature Phase Shift Keying.
8PSK	Phase Shift Keying.

Command Default

No default behavior or values

Command Modes

Satellite initial configuration

Command History

Release	Modification
12.3(14)T	This command was introduced.

Usage Guidelines

This command is typically used by an installation technician. Do not use this command unless your satellite service provider instructs you to perform the satellite initial configuration and provides all necessary parameter values.

Examples

The following example shows how to configure the VSAT modulation type:

```
Router(sat-init-config)# outbound modulation-type DVB
```

outbound sync ip address

To specify the outbound synchronization IP address, use the **outboundsyncipaddress** command in satellite initial configuration mode. To remove the outbound synchronization IP address configuration, use the **no** form of this command.

outbound sync ip address *address*
no outbound sync ip address

Syntax Description

address	Outbound synchronization IP address.

Command Default

No default behavior or values

Command Modes

Satellite initial configuration

Command History

Release	Modification
12.3(14)T	This command was introduced.

Usage Guidelines

This command is typically used by an installation technician. Do not use this command unless your satellite service provider instructs you to perform the satellite initial configuration and provides all necessary parameter values.

Examples

The following example shows how to configure the outbound synchronization IP address:

```
Router(sat-init-config)# outbound sync ip address 10.2.2.2
```

outbound viterbi-rate

To specify the VSAT Viterbi code rate, use the **outboundviterbi-rate** command in satellite initial configuration mode. To return to the default rate, use the **no** form of this command.

outbound viterbi-rate *rate*
no outbound viterbi-rate

Syntax Description

rate	Viterbi code rate. It can be one of the following values: • **1/2** • **1/4** • **2/3** • **3/4** • **3/4(2.05)** • **3/4(2.1)** • **3/4(2.6)** • **5/6** • **6/7** • **7/8** • **8/9**

Command Default

No default behavior or values

Command Modes

Satellite initial configuration

Command History

Release	Modification
12.3(14)T	This command was introduced.

Usage Guidelines

This command is typically used by an installation technician. Do not use this command unless your satellite service provider instructs you to perform the satellite initial configuration and provides all necessary parameter values.

Examples

The following example shows how to configure the VSAT Viterbi code rate:

```
Router(sat-init-config)# outbound viterbi-rate 3/4(2.6)
```

output

To enable out put of time of day messages using a 1PPS interface, use the **output** command in global configuration mode. To disable PTP output, use the **no** form of this command.

output 1pps *slot*/*bay* [**offset** *offset-value* [**negative**]] [**pulse-width** *pulse-amount* {**ns** | **us** | **ms**}]
no output 1pps *slot*/*bay* [**offset** *offset-value* [**negative**]] [**pulse-width** *pulse-amount* {**ns** | **us** | **ms**}]

Syntax Description

1pps	Configures the device to send 1 packet per second (1PPS) time of day messages using the RS422 port or 1PPS port. You can select 1PPS output with or without selecting a timing port.
slot	Slot of the 1PPS interface.
bay	Bay of the 1PPS interface.
offset	(Optional) Specifies an offset to compensate for a known phase error such as network asymmetry.
offset-value	Amount of offset in nanoseconds. The range is from 0 to 500,000,000.
negative	Specifies a negative offset 1PPS output value.
pulse-width	(Optional) Specifies a pulse width value.
pulse-amount	Amount of the pulse width. The range is from 1 to 4096. For 1PPS output using the RS422 port, you must specify a value of at least 2 ms.
ns	Specifies a pulse width value in nanoseconds.
us	Specifies a pulse width value in microseconds.
ms	Specifies a pulse width value in milliseconds.

Command Default

Time of day message output is not enabled.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(31)SB2	This command was introduced.
15.0(1)S	This command was integrated into Cisco IOS Release 15.0(1)S.
15.1(2)SNG	This command was implemented on the Cisco ASR 901 Series Aggregation Services Router.

Usage Guidelines

If you want to provide output frequency clock, configure this command in PTP mode. This command only applies to platforms that have 1PPS ports.

Examples

The following example shows how to configure output clocking:

```
Device> enable
Device# configure terminal
Device(config)# ptp clock ordinary domain 0
Device(config-ptp-clk)# output 1pps 3/0 offset 10 pulse-width 1000 ms
Device(config-ptp-clk)# end
```

The following example shows the time of day (ToD) configuration on the 1588V2 subordinate and corresponding output:

```
Device> enable
Device# config terminal
Device(config)# ptp clock ordinary domain 0
Device(config-ptp-clk)# tod 3/3 cisco
Device(config-ptp-clk)# output 1pps 0 250 ns
Device(config-ptp-clk)# clock-port SLAVE slave
```

Related Commands

Command	Description
input	Enables PTP input clocking using the 1.544 Mhz, 2.048 Mhz, or 10 Mhz timing interface or phase using the 1PPS or RS-422 interface.

overhead c2

To set the SONET path overhead bytes in the frame header to a specific standards requirement or to ensure interoperability with equipment from another vendor, use the **overhead** command in SONET path configuration mode. To remove the setting of the SONET path overhead bytes from the configuration file and restore the system to its default condition, use the **no** form of this command.

overhead c2 *value*

no overhead c2 *value*

Syntax Description

Syntax Description

c2 *value*	Configures the C2 byte in the Path OverHead (POH) to indicate the contents of the payload inside the frame. C2 byte is to communicate the payload type that the SONET Framing OverHead (FOH) encapsulates.

Command Modes

Controller configuration

Command History

Release	Modification
XE 3.18SP	Support for this command was introduced on NCS 4200 Series.
XE Everest 16.5.1	This command was introduced on the Cisco ASR 920 Routers and Cisco NCS 4200 Series.

Usage Guidelines

This command is used to configure C2 flag as the path overhead.

Examples

The following example shows the configuration of C2 flag:

```
enable
configure terminal
controller MediaType 0/5/0
mode sonet
controller sonet 0/5/0
sts-1 1
overhead c2 10
end
```

Related Commands

Command	Description
controller sonet	Configures the SONET mode.
show controller sonet	Displays SONET controller configuration.

overhead j0

To specify the Regenerator Section (RS) Trace identifier (J0), use the **overheadj0** command in controller configuration mode. To restore the default value, use the **no** form of this command.

overhead j0 {**transmit** | **receive**} *string*
no overhead j0 {**transmit** | **receive**} *string*

Syntax Description

For NCS 4200 Series:

overhead j0 {*expected* | *tx*} [**length** *number* | **tracebuffer** *string*]

transmit	Specifies that the *string* argument is sent on the transmit line.
receive	Specifies that the configured *string* argument is matched with the string received from a peer.
string	Value in the range from 0 to 255 that is converted into character format and embedded in a 16-byte frame. The default is 1.
expected	Configures the expected trace identifier of the controller.
tx	Configures the packets transmitted.
length *number*	Specifies the length of the expected trace identifier.
tracebuffer *string*	Configures the SONET path trace buffer. Enters the ACSII text for the controller.

Command Default

The default value is 1, and no peer authentication is performed.

Command Modes

Controller configuration

Command History

Release	Modification
12.0(17)S	This command was introduced.
12.2(15)T	This command was integrated into Cisco IOS Release 12.2(15)T, and the **transmit** and **receive** keywords were added.
XE 3.18SP	Support for this command was introduced on NCS 4200 Series.

Usage Guidelines

RS trace is a maintenance feature of SONET. One byte (J0) of the Section overhead associated with each SONET frame is used to carry information identifying the transmitting equipment.

Use this command for peer authentication and continuity testing between two STM-1 optical peers. If the authentication string sent by the originating peer does not match the configured string on the receiving peer, the SONET controller will not come up on the receiving peer. Alarm logs on the originating peer will show that it has RS-Trace Identifier Mismatch (RS-TIM).

For NCS 4200 Series, use this command to configure line and section overhead of SONET line.

Examples

The following example shows how to configure J0 overhead in both the transmit and receive directions on a STM-1 trunk card:

```
Router(config)# controller sonet 2/0
Router(config-controller)# overhead j0 transmit 22
Router(config-controller)# overhead j0 receive 34
```

The following example shows how to set the RS Trace identifier to 82:

```
Router(config-controller)# overhead j0 transmit 82
```

Examples

For NCS 4200 Series, the following example shows how to configure line and section overhead:

```
enable
configure terminal
controller Mediatype 0/5/0
controller sonet 0/5/0
overhead j0 tx length 1-byte
end
```

Related Commands

Command	Description
controller sonet	Configures the SONET mode.
show controller sonet	Displays SONET controller configuration.

overhead j1

To configure the message length and the message text of the High Order Path Trace identifier (J1), use the **overheadj1** command in controller configuration or path configuration mode. To restore the default value, use the **no** form of this command.

overhead j1 length {**16** | **64**} {**transmit-message** | **receive-message**} *string*
no overhead j1 length {**16** | **64**} {**transmit-message** | **receive-message**} *string*

Syntax Description

For NCS 4200 Series, use the following command:

overhead j1 [**expected** | **tx**] [**length** | **message**]

length	Specifies the length of the authentication *string* argument.
16	Specifies that the length of the authentication *string*is 16 characters. The STM-1 trunk card supports a string length of 16.
64	Specifies that the length of the authentication *string*is 64 characters.
transmit-message	Specifies that the *string* argument is sent on the transmit line.
receive-message	Specifies that the configured *string* argument is matched with the string received from a peer.
string	Combination of characters and numbers for the specified **length** value.
tx	Configures the packets transmitted.
expected	Configures the expected trace identifier of the controller.

Command Default

The default message length is 16 for SDH framing and 64 for SONET framing. No peer authentication is performed.

Command Modes

Controller configuration

Path configuration

Command History

Release	Modification
12.0(17)S	This command was introduced.
12.2(15)T	This command was integrated into Cisco IOS Release 12.2(15)T, and the **transmit-message** and **receive-message** keywords were added.

Usage Guidelines

Path trace is a maintenance feature of SONET/SDH. One byte (J1) of the Path overhead associated with each path in the SONET/SDH frame is used to carry information identifying the originating Path Terminating Equipment (PTE).

Where you configure the Path Trace identifier depends on the framing (SDH or SONET) and the AUG mapping. In SDH with AU-4 mapping, the Path Trace identifier is configured at the SONET controller level. In SDH with AU-3 mapping or in SONET framing, the Path Trace identifier is configured at the path level.

In accordance with SONET and SDH standard requirements, the Path Trace message you enter is manipulated as follows:

- If you select a message length of 16, the actual message length can be up to 15 characters. An additional byte, prepended to the message, contains the result of a CRC7 calculated on the message. If the actual message text is fewer than 15 characters, the message text is padded to its full length with NULL characters.
- If you select a message length of 64 and the actual message text is fewer than 62 characters, the message text is padded with NULL characters. The last two byte positions, 63 and 64, are always CR/LF (0x0D/0x0A).

Use this command for peer authentication and continuity testing between two STM-1 optical peers. If the authentication string sent by the originating peer does not match the configured string on the receiving peer, the Path (and all E1 controllers within the path) will not come up on the receiving peer. Alarm logs on the originating peer will show that it has High Order Path-Trace Identifier Mismatch (HP-TIM).

Examples

The following example shows J1 configuration in SDH framing with AU-4 AUG mapping. The **overheadj1**command sets the message length to 16, and specifies the message text as metro_SF:

```
Router(config-controller)# au-4 1
Router(config-ctrlr-au4)# overhead j1 length 16 transmit-message metro_SF
```

The following example shows J1 configuration in SDH framing with AU-3 AUG mapping. The **overheadj1** command sets the message length to 16, and specifies the message text as metro_LA:

```
Router(config)# controller sonet 4/0Router(config-controller)# au-3 3
Router(config-ctrlr-au3)# overhead j1 length 16 receive-message metro_L
```

The following example shows J1 configuration in SONET framing in STS-1 mode. The **overheadj1** command sets the message length to 64, and specifies the message text:

```
Router(config)# controller sonet 4/0
Router(config-controller)# sts-1 3
Router(config-ctrlr-sts1)# overhead j1 length 64 transmit-message metro_washington
gsr_0057/4/3
```

The following example shows how to configure j1 overhead in both the transmit and receive directions:

```
Router(config)# controller sonet 2/0
Router(config-controller)# overhead j1 length 2 transmit-message 22
Router(config-controller)# overhead j1 length 2 receive-message 34
```

Examples

For NCS 4200 Series, the following example shows the configuration of J1 flag:

```
enable
configure terminal
controller sonet 0/5/0
sts-1 1
overhead j1 message word
end
```

overhead tunnel

To configure a transparent overhead tunnel on SDH or SONET controller, use the **overhead tunnel** command in the controller mode. To remove the tunnel from SDH or SONET controller, use the **no** form of this command.

For SONET

overhead tunnel {**all** | **sdcc** | **ldcc** | **k1k2** | **loh** | **soh** } **cem-group** *cem-id* **unframed**

For SDH

overhead tunnel {**all** | **ms-dcc** | **rs-dcc** | **k1k2** | **loh** | **soh** } **cem-group** *cem-id* **unframed**

Syntax Description

Syntax Description

all	Specify to include all section and line headers.
sdcc	Specify to include D1, D2, and D3 section header bytes for SONET.
ms-dcc	Specify to include D1, D2, and D3 section header bytes for SDH.
ldcc	Specify to include D4 to D12 line header bytes for SONET.
rs-dcc	Specify to include D4 to D12 line header bytes for SDH.
k1k2	Specify to include K1 and K2 line header bytes.
loh	Specify to include K1, K2, and D4 to D12, E2 line header bytes.
soh	Specify to include E1, F1, D1, D2, and D3 line header bytes.
cem-id	Specify CEM ID configured for the CEM group.

Command Default

None

Command Modes

Configuration mode

Command History

Release	Modification
Cisco IOS XE 16.9.x	Support for this command was introduced on ASR 900 Series.

Usage Guidelines

Before creating transparent overhead tunnel, ensure that you perform the following steps:

- Set mode under STS path before enabling overhead tunnel.
- Mode and TOH type should be same on both PEs in an end-to-end setup.

For more information on prerequisites for transparent overhead tunnel, see 1-Port OC-192 or 8-Port Low Rate CEM Interface Module Configuration Guide, Cisco IOS XE Everest 16.8.x (Cisco ASR 900 Series).

Examples

The following example shows how to configure transparent overhead tunnel on the SONET controller:

```
router(config)#controller sonet 0/7/7
```

```
router(config-controller)#overhead tunnel SDCC cem-group100 unframed
router(config-controller)#end
```

To configure transparent overhead tunnel pseudowire, use the following commands:

```
router(config)#interface cem 0/7/7
router(config-if)#cem  100
router(config-if)#xconnect  203.0.113.1  130  encapsulation MPLS
router(config-controller)#end
```

Related Commands

Command	Description
show cem circuit interface cem *interface-name*	Displays CEM interface configured for transparent overhead tunnel.

overhead s1s0

To set the SONET path overhead bytes in the frame header to a specific standards requirement or to ensure interoperability with equipment from another vendor, use the **overhead** command in SONET path configuration mode. To remove the setting of the SONET path overhead bytes from the configuration file and restore the system to its default condition, use the **no** form of this command.

overhead s1s0 *value*

no overhead s1s0 *value*

Syntax Description

Syntax Description

s1s0 *value*	Sets the SS bits value of the H1 byte in the SONET line overhead. For SONET mode, use 0 (this is the default).

Command Modes

Controller configuration

Command History

Release	Modification
XE 3.18SP	Support for this command was introduced on NCS 4200 Series.

Usage Guidelines

Use the **overhead** command to set the SONET overhead bytes in the frame header to a specific standards requirement. This command is used to configure line and section overhead.

Examples

The following example shows the configuration of overhead s1s0:

```
enable
configure terminal
controller MediaType 0/5/0
mode sonet
controller sonet 0/5/0
overhead s1s0 2
overhead j0 tx-length 1-byte
end
```

Related Commands

Command	Description
controller sonet	Configures the SONET mode.
show controller sonet	Displays SONET controller configuration.

password (satellite initial configuration)

To define or to change the password of the NM-1VSAT-GILAT network module required to enter satellite initial configuration mode, use the **password** command in the satellite initial configuration mode.

password *password*

Syntax Description

password	A string of up to 32 alphanumeric characters.

Command Default

The factory-supplied default password is active.

Command Modes

Satellite initial configuration.

Command History

Release	Modification
12.4(11)XJ2	This command was introduced.
12.4(15)T	This command was integrated into Cisco IOS Release 12.4(15)T.

Usage Guidelines

The NM-1VSAT-GILAT network module has a factory-supplied unique default password to enter satellite initial configuration mode for initial configuration. During this configuration, the **password** command is used to set a user-defined password for subsequent entries to satellite initial configuration mode. The user-defined password consists of up to 32 alphanumeric characters.

Examples

The following example shows how to enter a user-defined password:

```
Router(sat-init-config)# password vsatuser
```

payload-compression

To enable payload compression, use the **payload-compression**command in CEM configuration mode. To disable payload compression, use the **no** form of this command.

payload-compression
no payload-compression

Syntax Description

This command has no arguments or keywords.

Command Default

Payload compression is disabled by default.

Command Modes

CEM configuration

Command History

Release	Modification
12.3(7)T	This command was introduced.

Usage Guidelines

Payload compression can be enabled only for a maximum of 3 Mbps per network module.

Examples

The following example demonstrates how to enable payload compression.

```
Router(config-cem)# payload-compression
```

Related Commands

Command	Description
cem	Enters circuit emulation configuration mode.
payload-size	Configures payload size.
show cem	Displays CEM statistics.

payload-size dejitter-buffer

To configure the size of payload and dejitter-buffer of a circuit emulation (CEM) over MPLS, use the **payload-size dejitter-buffer** command in CEM configuration mode. To restore the default the size, use the **no** form of this command.

payload-size *size* **dejitter-buffer** *size*

no payload-size *size* **dejitter-buffer** *size*

size	The payload-size is the integer that defines the number of bytes per packet. Range of payload-size is from 64 to 1312. Range for dejitter-buffer size from 1 to 256 milliseconds. For T1, the valid values of payload size are 32 to 512. The default payload-size is 192 bytes and dejitter-buffer size is 5 milliseconds. For T3 clear channel, the default payload-size is 1024 bytes and dejitter-buffer size is 5 milliseconds. For T3 channelized, the default payload-size is 192 bytes and dejitter-buffer size is 5 milliseconds. For E1, the valid values of payload size are 64 to 1312. The default payload-size is 256 bytes and dejitter-buffer size is 5 milliseconds.

Command Default

The dejitter-buffer defaults to 5 milliseconds.

Command Modes

CEM configuration

Command History

Command History

Release	Modification
XE 3.18SP	This command was introduced.
XE Everest 16.5.1	This command was implemented on the Cisco ASR 900 Series Routers and Cisco NCS 4200 Series.

Usage Guidelines

Use this command to configure the size of each CEoIP packet. Smaller sizes reduce delay but diminish efficiency.

Note The payload size must be a multiple of the number of time slots and 16. The payload size you enter will automatically change to match the above requirement, and a console message will inform you the change. When you select a value of payload-size, the acceptable range of dejitter-buffer is displayed.

Examples

The following example shows how to set the payload size as 1024 and dejitter buffer to 10 milliseconds.

```
Router(config-controller)# payload-size 1024 dejitter-buffer 10
```

Related Commands

Command	Description
cem	Enters circuit emulation configuration mode.

payload-size

To configure the payload size of a circuit emulation (CEM) over IP (CEoIP) packet, use the **payload-size**command in CEM configuration mode. To restore the default payload size, use the **no** form of this command.

payload-size *size*
no payload-size

Syntax Description

size	Integer that defines the number of bytes per CEoIP packet. Range is from 1 to 1312. The maximum configurable payload size is as follows: • 1312 bytes if data protection is not enabled • 656 bytes if data protection is enabled The minimum configurable payload size for an unframed T1 or E1 channel is 256 bytes. The minimum configurable payload size for a framed T1 or E1 channel is as follows: • 56 bytes if the data rate is less than or equal to 256,000 kbps • 128 bytes if the data rate is greater than 256,000 kbps and less than or equal to 512,000 kbps • 256 bytes if the data rate is greater than 512,000 kbps The minimum configurable payload size for a serial channel is as follows: • 1 byte if the data rate is less than or equal to 2400 kbps • 4 bytes if the data rate is greater than 2400 kbps but less than or equal to 9600 kbps • 16 bytes if the data rate is greater than 9600 kbps but less than or equal to 32,000 kbps • 32 bytes if the data rate is greater than 32,000 kbps but less than or equal to 64,000 kbps • 64 bytes if the data rate is greater than 64,000 kbps but less than or equal to 256,000 kbps • 128 bytes if the data rate is greater than 256,000 kbps but less than or equal to 512,000 kbps • 256 bytes if the data rate is greater than 512,000 kbps **Note** For T1 and E1, the integer must be a multiple of the number of time slots and 16. For Cisco ASR 901 Series Aggregation Services Routers, the value specifies the size of the payload for packets on a structured CEM channel. Valid values are 32 to 512. The default payload size for a T1 channel is 192 bytes and for an E1 channel is 256 bytes. The default payload size is calculated by multiplying 8 by the number of timeslots and then multiplying the result by 1 ms packetization delay.

Command Default

The default payload size for a serial channel is 32 bytes. Defaults for T1 and E1 channels are shown in the tables below.

*Table 1: Default Payload Size for N*64-kbps T1/E1 Channels*

Number of Time Slots	Channel Data Rate (kbps)	Default Payload Size (bytes)
1	64	64
2	128	64
3	192	96
4	256	64
5	320	160
6	384	144
7	448	224
8	512	128
9	576	288
10	640	320
11	704	352
12	768	288
13	832	416
14	896	336
15	960	480
16	1024	256
Unframed T1	1544	512
Unframed E1	2048	512
17	1088	544
18	1152	576
19	1216	608
20	1280	560
21	1344	672
22	1408	528
23	1472	736
24	1536	528
25	1600	800

Number of Time Slots	Channel Data Rate (kbps)	Default Payload Size (bytes)
26	1664	624
27	1728	864
28	1792	560
29	1856	928
30	1920	720
31	1984	992

*Table 2: Default Payload Size for N*56-kbps T1 Channels*

Number of Time Slots	Channel Data Rate (kbps)	Default Payload Size (bytes)
1	56	56
2	112	56
3	168	168
4	224	56
5	280	280
6	336	168
7	392	168
8	448	168
9	504	504
10	560	280
11	616	616
12	672	336
13	728	728
14	784	280
15	840	840
16	896	336
17	952	952
18	1008	1008
19	1064	1064

Number of Time Slots	Channel Data Rate (kbps)	Default Payload Size (bytes)
20	1120	560
21	1176	672
22	1232	616
23	1288	1288
24	1344	672

Cisco ASR 901 Series Aggregation Services Routers

The default payload size for a structured CEM channel depends on the number of timeslots that constitute the channel.

Command Modes

- CEM configuration (config-if-cem)
- CEM circuit configuration (config-if-cem)

Command History

Release	Modification
15.1(2)SNG	This command was implemented on Cisco ASR 901 Series Aggregation Services Routers.
15.1(2)SNG	This command was implemented on Cisco ASR 901 Series Aggregation Services Routers.

Usage Guidelines

Use this command to configure the size of each CEoIP packet. Smaller sizes reduce delay but diminish efficiency.

Note The payload size must be a multiple of the number of time slots and 16. The payload size entered by the user will be automatically changed to match the above requirement, and a console message will inform the user of this change.

The Cisco ASR 901 series router only supports a payload size of 486 (625 packets per second) or 243 (1250 packets per second).

Examples

The following example shows how to configure a payload size of 224.

```
Router(config-cem)# payload-size 224
```

Related Commands

Command	Description
cem	Enters circuit emulation configuration mode.
payload-compression	Enables payload compression.
payload-compression	Enables payload compression.

Command	Description
payload-compression	Enables payload compression.
show cem	Displays CEM channel statistics.

physical-interface

To create a physical subinterface and to associate it with the Virtual Multipoint Interface (VMI) on a router, use the **physical-interface** command in interface configuration mode. To return to the default mode, use the **no** form of this command.

physical-interface *interface-type / slot*
no physical-interface *interface-type / slot*

Syntax Description

interface-type	Type of interface or subinterface.
/ *slot*	Slot in which the interface is present.

Command Default

No physical interface exists.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.4(15)XF	This command was introduced.
12.4(15)T	This command was integrated into Cisco IOS Release 12.4(15)T to support VMIs in Mobile Adhoc Router-to-Radio Networks.
12.4(24)T	This command was modified. This command supports the subinterfaces and VLANS associated with an interface.

Usage Guidelines

The **physical-interface** command supports the subinterfaces and VLANs associated with an interface. This command also allows VMI interface to operate over encapsulated interfaces, if required. Only one physical interface can be assigned to a VMI interface. Because there is very high number of VMI interfaces that can be used, assign a new VMI for each physical interface.

Examples

The following example shows how to create a physical subinterface:

```
Router(config)# interface vmi1
Router(config-if)# physical-interface FastEthernet0/1
```

Related Commands

Command	Description
debug vmi	Displays debugging output for VMIs.
eigrp interface	Sets a threshold value to minimize hysteresis in a router-to-radio configuration.
interface vmi	Creates a VMI interface.
mode bypass	Enables VMIs to support multicast traffic

physical-layer

To specify the mode of a slow-speed serial interface on a router as either synchronous or asynchronous, use the **physical-layer** command in interface configuration mode. To return the interface to the default mode of synchronous, use the **no** form of this command.

physical-layer {**sync** | **async**}
no physical-layer

Syntax Description

sync	Places the interface in synchronous mode. This is the default.
async	Places the interface in asynchronous mode.

Command Default

Synchronous mode

Command Modes

Interface configuration

Command History

Release	Modification
11.2	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

This command applies only to low-speed serial interfaces available on Cisco 2520 through Cisco 2523 series routers.

In synchronous mode, low-speed serial interfaces support all interface configuration commands available for high-speed serial interfaces, except the following two commands:

- **half-duplex timer cts-delay**
- **half-duplex timer rts-timeout**

When placed in asynchronous mode, low-speed serial interfaces support all commands available for standard asynchronous interfaces.

When you enter this command, it does not appear in the output of **moresystem:running-config** and **morenvram:startup-config** commands because the command is a physical-layer command.

Examples

The following example shows how to change a low-speed serial interface from synchronous to asynchronous mode:

```
Router(config)# interface serial 2
Router(config-if)# physical-layer async
```

Related Commands

Command	Description
more	Displays a specified file.

platform console

To select the console that is used to access the virtual router interface, use the **platform console** command in global configuration mode.

platform console {**serial** | **virtual**}

Syntax Description

serial	Specifies that the virtual router is accessed using the virtual serial port on the ESXi host.
virtual	Specifies that the virtual router is accessed using the VMware VM console.

Command Default

No default.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE 3.8S (Controlled Availability)	This command was introduced on the Cisco CSR 1000V Cloud Services Router.

Usage Guidelines

During the first-time installation and bootup of the virtual router, you choose whether to access the virtual router using the VM console or the virtual serial port on the ESXi host. The default setting is to use the VM console.

This command is used for changing the console access to the virtual router after first-time installation and bootup. After you enter the command, you must reload or power-cycle the router in order for the new setting to take effect.

Examples

The following example configures the virtual router to be accessed through the VM console:

```
Router> enable
Router# configure terminal
Router(config)# platform console virtual
Router(config)# end
Router# copy system:running-config nvram:startup-config
Router# reload
```

The following example configures the virtual router to be accessed through the virtual serial port:

```
Router> enable
Router# configure terminal
Router(config)# platform console serial
Router(config)# end
Router# copy system:running-config nvram:startup-config
Router# reload
```

platform cwan acl software-switched

To allow ACLs to be applied to packets that are software-switched between WAN cards and the route processor, use the **platformcwanaclsoftware-switched**command in global configuration mode. To have ACLs applied only to packets that are hardware-switched between WAN cards and the route processor, use the **no** form of this command.

platform cwan acl software-switched {**egress** | **ingress**}
no platform cwan acl software-switched {**egress** | **ingress**}

Syntax Description

egress	Allows ACLs to be applied to software-switched egress WAN packets.
ingress	Allows ACLs to be applied to software-switched ingress WAN packets.

Command Default

ACLs are not applied to packets that are software-switched between WAN cards and the route processor. ACLs are applied only to packets that are hardware-switched between WAN cards and the route processor.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(50)SY	This command was introduced.
12.2(33)SXI2	This command was integrated into Cisco IOS Release 12.2(33)SXI2.

Usage Guidelines

By default, software-switched WAN packets are not subjected to ACL lookup in the ACL TCAM and are therefore not affected by hardware-only features. As a result, VACL capture will fail for software-switched WAN packets. The **platformcwanaclsoftware-switched**command allows ACLs to be applied to ingress or egress software-switched WAN packets.

When you use the **platformcwanaclsoftware-switched**command to allow VACL capture, these limitations apply:

Note The **platformcwanaclsoftware-switched**command is ignored by the SIP-600. Ingress software-switched packets on the SIP-600 are not subjected to ACL lookups, and VACL features are not supported.

Examples

This example shows how to enable ACLs for software-switched ingress WAN packets:

```
Router(config)#
platform cwan acl software-switched ingress
```

Related Commands

Command	Description
show platform acl software-switched	Displays whether ACLs are enabled for software-switched WAN packets.

platform enable controller mediaType

Use this command to to enable a particular license type on the controller port. Providing a particular license type is mandatory to enable the license on the IM.

platform enable controller Mediatype <*slot/bay/port*> <*port rate*>

Syntax Description

Syntax Description:

slot	Physical slot number of the interface
bay	Bay of the interface
port	Mediatype port number
port rate	Rate configured on the port

Command Default

None

Command Modes

Global configuration

Command History

Release	Modification
XE Everest 16.7.1	This command was integarted into the Cisco NCS 4200 Series, Cisco ASR 900 Series, and Cisco ASR 920 Routers.

Usage Guidelines

License enabling is allowed when the license with the same rate is configured on the port. The configuration fails if the license with a different rate is configured on the port.

Examples

The following example shows how to enable the license:

```
enable
configure terminal
platform enable controller MediaType 0/4/16 oc3
controller MediaType 0/4/16
mode sonet
exit
controller sonet 0/4/16
rate oc3
exit
```

Related Commands

Command	Description
show license detail	Verifies the license configuration.

platform hardware throughput crypto

To configure a throughput value on a physical router, use the **platform hardware throughput crypto** command in global configuration mode. To revert to the default value, use the **no** form of this command.

platform hardware throughput crypto { *throughput-value* }

no platform hardware throughput crypto

Syntax Description

throughput-value	Enter a throughput value. Use the question mark (?) online help function to display the available values. The available options vary depending on the device.

Command Default

The device-specific default throughput level is effective.

PID	Default Throughput
C8300-1N1S-4T2X	10 Mbps
C8300-2N2S-6T	10 Mbps
C8300-1N1S-6T	10 Mbps
C8300-2N2S-4T2X	10 Mbps
C8200-1N-4T	10 Mbps
C8200-1N-4T-L	10 Mbps
C8500-12X4QC	2.5 Gbps
C8500-12X	2.5 Gbps
C8500L-8S4X	2.5 Gbps
C8500-20X6C	T4

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Amsterdam 17.3.2	This command was introduced on Cisco Catalyst 8300, and 8500 Series Edge Platforms.
Cisco IOS XE Bengaluru 17.4.1	This command was introduced on the Cisco Catalyst 8200 Series Edge Platforms.

Usage Guidelines

Before you configure a throughput level, take note of these aspects:

- Ensure that you have configured a boot-level license. Otherwise **platform hardware throughput crypto** is not recognized as a valid command, on the command line interface. For information about configuring a boot-level license, see Configuring a Boot Level License.

- The throughput you are entitled to. This is a value that is represented in the License product ID (PID) when you order a Cisco DNA license. It can be a numeric throughput value, such as DNA-C-**10M**-E-3Y, or a tier-based throughput value, such as DNA-C-**T0**-E-3Y.

  Support for tier-based throughput configuration was introduced in Cisco IOS XE Cupertino 17.7.1a. Use the question mark (?) online help function to display the available tier-based *and* numeric throughput values. Refer to Tier and Numeric Throughput Mapping for Physical Platforms, Cisco IOS XE Cupertino 17.8.1a and Later Releases to know the numeric equivalent of a tier.

- If you are configuring throughput greater than 250 Mbps, ensure that you have installed a Smart Licensing Authorization Code (SLAC). Options greater than 250 Mbps are displayed only if SLAC is installed. For information about installing SLAC, see Manually Requesting and Auto-Installing a SLAC.

Support for aggregate throughput throttling was introduced in Cisco IOS XE Cupertino 17.8.1a. With this, when you configure throughput levels greater than 250 Mbps or Tier 2 and higher tiers on physical devices, aggregate throughput throttling is effective. *Aggregate throughput is double the bidirectional throughput*.

When aggregate throughput throttling is effective, throttling is not applied to transmitted (Tx) and received (Rx) traffic separately, rather, any ratio within the aggregate throughput limit applies. For example, If you configure a throughput of 500 Mbps on a device, a maximum of 1 Gbps transmitted (Tx) traffic and 0 Mbps received (Rx) traffic, or, 100 Mbps Tx and 900 Mbps Rx, or any other ratio within the aggregate 1 Gbps throughput limit, is supported. For more information and examples, see Throughput as a Numeric Value and Throughput as a Tier.

To display throughput information, enter the **show platform hardware throughput crypto** command in privileged EXEC mode.

The following example shows you how to configure a tier-based throughput value.

Displaying current configuration:

```
Device# show platform hardware throughput crypto
show platform hardware throughput crypto
Current configured crypto throughput level: 250M
     Level is saved, reboot is not required
Current enforced crypto throughput level: 250M
Crypto Throughput is throttled at 250M
Default Crypto throughput level: 10M
Current boot level is network-premier
```

Verifying SLAC is installed before configuring a throughput level greater than 250 Mbps or Tier 2 and higher tiers:

```
Device# show license authorization
Overall status:
  Active: PID:C8300-2N2S-4T2X,SN:FDO2250A0J5
      Status: SMART AUTHORIZATION INSTALLED on Mar 02 05:05:19 2022 UTC
      Last Confirmation code: 418b11b3

Authorizations:
  Router US Export Lic. for DNA (DNA_HSEC):
    Description: U.S. Export Restriction Compliance license for
    DNA based Routers
    Total available count: 1
    Enforcement type: EXPORT RESTRICTED
    Term information:
      Active: PID:C8300-1N1S-4T2X,SN:FDO2250A0J5
        Authorization type: SMART AUTHORIZATION INSTALLED
        License type: PERPETUAL
          Term Count: 1
```

```
Purchased Licenses:
  No Purchase Information Available
```

Configuring a tier-based throughput value from the list of available values for this device:

```
Device# configure terminal
Device(config)# platform hardware throughput crypto ?
  100M  100 mbps bidirectional thput
  10M   10 mbps bidirectional thput
  15M   15 mbps bidirectional thput
  1G    2 gbps aggregate thput
  2.5G  5 gbps aggregate thput
  250M  250 mbps bidirectional thput
  25M   25 mbps bidirectional thput
  500M  1gbps aggregate thput
  50M   50 mbps bidirectional thput
  T0    T0(up to 15 mbps) bidirectional thput
  T1    T1(up to 100 mbps) bidirectional thput
  T2    T2(up to 2 gbps) aggregate thput
  T3    T3(up to 5 gbps) aggregate thput

Device(config)# platform hardware throughput crypto T2
% These values don't take effect until the next reboot.
Please save the configuration.
*Mar 02 05:06:19.042: %CRYPTO_SL_TP_LEVELS-6-SAVE_CONFIG_AND_RELOAD:
New throughput level not applied until reload; please save config
```

Saving configuration to ensure changes persist across reloads and reloading the device:

```
Device# exit
Device# copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
Device# reload
Proceed with reload? [confirm]
*Mar 02 05:07:00.979: %SYS-5-RELOAD: Reload requested by console.
Reload Reason: Reload Command.
```

Displaying configuration again:

```
Device# show platform hardware throughput crypto
Current configured crypto throughput level: T2
     Level is saved, reboot is not required
Current enforced crypto throughput level: 1G
Crypto Throughput is throttled at 2G(Aggregate)
Default Crypto throughput level: 10M
Current boot level is network-premier
```

Related Commands

Command	Description
show platform hardware throughput crypto	Displays throughput information on a physical router.

platform hardware throughput level

To change the maximum throughput level on the virtual router, use the **platform hardware throughput level** command in global configuration mode. To return the platform throughput level to the default value, use the **no** form of this command.

Cisco IOS XE Release 3.9S:

platform hardware throughput level {**10000** | **25000** | **50000** | **eval-only**}

Cisco IOS XE Release 3.10S and Later:

platform hardware throughput level MB {**10** | **100** | **1000** | **25** | **250** | **50** | **500**}

Syntax Description

Cisco IOS XE Release 3.9S:	
10000	Sets the maximum throughput to 10,000 Kbps (10 Mbps).
25000	Sets the maximum throughput to 25,000 Kbps (25 Mbps).
50000	Sets the maximum throughput to 50,000 Kbps (50 Mbps).
eval-only	Specifies to use the maximum throughput for the evaluation license only.
Cisco IOS XE Release 3.10S:	
10	Sets the maximum throughput to 10 Mbps.
100	Sets the maximum throughput to 100 Mbps.
1000	Sets the maximum throughput to 1 Gbps.
25	Sets the maximum throughput to 25 Mbps.
250	Sets the maximum throughput to 250 Mbps.
50	Sets the maximum throughput to 50 Mbps.
500	Sets the maximum throughput to 500 Mbps.

Command Default

The default maximum throughput level is determined by the installed base license.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Release 3.9S	This command was introduced on the Cisco CSR 1000V Series Cloud Services Router.
Cisco IOS XE 3.10S	The command was updated to change the keywords to units in Mbps, and support for maximum throughput values of 100 Mbps, 250 Mbps, 500 Mbps, and 1 Gbps was added.

Usage Guidelines

The Cisco CSR 1000V requires the installation of base licenses that set the maximum throughput of the platform.

Depending on the configuration and the licenses installed, you may need to manually increase or decrease the maximum throughput level on the Cisco CSR 1000V. The maximum throughput on the router before the license is activated, or if the license is invalidated, is 2.5 Mbps. When you install the base subscription license and accept the EULA, the maximum throughput on the Cisco CSR 1000V will increase to the level allowed by the license.

You may need to manually change the maximum throughput level in the following cases:

- If you are using an evaluation license. When the evaluation license is first installed, the maximum throughput is limited to 2.5 Mbps before the license is activated. You must accept the EULA and enter the **platform hardware throughput level**command to increase the maximum throughput. When the 60-day evaluation license expires, the maximum throughput level reverts to 2.5 Mbps.
- If you want to reduce the maximum throughput level from the maximum permitted by the installed licenses. For example, if you have the 50-Mbps license installed and you want to reduce the maximum throughput to 25 Mbps. You must enter the **platform hardware throughput level** command to reduce the maximum throughput.
- If you previously changed the maximum throughput using the **platform hardware throughput level** command. When you enter the command, it becomes part of the configuration file. You must enter the command again to change the maximum throughput level.

When changing the maximum throughput level, you do not need to reboot the Cisco CSR 1000V for the change to take effect. If you try to increase the throughput level higher than what the installed license supports, you will receive an error message.

Example

The following example changes the maximum throughput level to 500 Mbps:

```
Router(config)# platform hardware throughput level MB 500
```

The following example changes the maximum throughput level to the default level supported by the installed license:

```
Router(config)# no platform hardware throughput level
```

Related Commands

Command	Description
show platform hardware throughput level	Displays the current maximum throughput level for a virtual router.

platform ip features sequential

To enable Internet Protocol (IP) precedence-based or differentiated services code point (DSCP)-based egress quality of service (QoS) filtering to use any IP precedence or DSCP policing or marking changes made by ingress policy feature card (PFC) QoS, use the **platformipfeaturessequential** command in interface configuration mode. To return to the default settings, use the **no** form of this command.

platform ip features sequential [**access-group** {*ip-acl-nameip-acl-number*}]
no platform ip features sequential [**access-group** {*ip-acl-nameip-acl-number*}]

Syntax Description

access-group *ip-acl-name*	(Optional) Specifies the name of the ACL that is used to specify the match criteria for the recirculation packets.
access-group *ip-acl-number*	(Optional) Specifies the number of the ACL that is used to specify the match criteria for the recirculation packets; valid values are from 1 to 199 and from 1300 to 2699.

Command Default

IP precedence-based or DSCP-based egress QoS filtering uses received IP precedence or DSCP values and does not use any IP precedence or DSCP changes made by ingress QoS as the result of policing or marking.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.2(50)SY	This command was introduced.
12.2(18)SXE	Support for this command was introduced on the Supervisor Engine 720.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines



Caution If the switch is operating in PFC3A mode with egress ACL support for remarked DSCP configured, when the PFC3 processes traffic to apply ingress PFC QoS, it applies ingress PFC QoS filtering and ingress PFC QoS, and incorrectly applies any egress QoS filtering and egress PFC QoS configured on the ingress interface, which results in unexpected behavior if QoS filtering is configured on an interface where egress ACL support for remarked DSCP is enabled. This problem does not occur in other PFC3 modes.

The enhanced egress-QoS filtering enables the IP precedence-based or DSCP-based egress-QoS filtering to use any IP precedence or DSCP policing or marking changes made by ingress QoS.

The nonenhanced egress-QoS filtering behavior is the normal Cisco 7600 series router or the Catalyst 6500 series switch behavior when QoS is applied in the hardware.

The PFC3 provides egress PFC QoS only for Layer 3-switched and routed traffic on egress Layer 3 interfaces (either LAN ports configured as Layer 3 interfaces or VLAN interfaces).

You configure enhanced egress QoS filtering on ingress Layer 3 interfaces (either LAN ports configured as Layer 3 interfaces or VLAN interfaces).

To enable enhanced egress QoS filtering only for the traffic filtered by a specific standard, extended named, or extended numbered IP ACL, enter the IP ACL name or number.

If you do not enter an IP ACL name or number, enhanced egress QoS filtering is enabled for all IP ingress IP traffic on the interface.



Note When you configure enhanced egress-QoS filtering, the PFC3A processes traffic to apply ingress PFC QoS. The PFC3A applies ingress-QoS filtering and Cisco 7600 series router or the Catalyst 6500 series switch hardware ingress QoS. The PFC3A incorrectly applies any egress-QoS filtering and Cisco 7600 series router or the Catalyst 6500 series switch hardware egress QoS that is configured on the ingress interface.



Note If you configure enhanced egress-QoS filtering on an interface that uses Layer 2 features to match the IP precedence or DSCP as modified by ingress-QoS marking, the packets are redirected or dropped and prevented from being processed by egress QoS.



Note If you enable enhanced egress-QoS filtering, the hardware acceleration of NetFlow-based features such as reflexive ACL, NAT, and TCP intercept are disabled.

To verify configuration, use the **showrunning-configinterface** command.

Examples

The following example shows how to enable enhanced egress-QoS filtering:

```
Router(config-if)# platform ip features sequential

Router(config-if)#
```

The following example shows how to disable enhanced egress-QoS filtering:

```
Router(config-if)# no platform ip features sequential

Router(config-if)#
```

Related Commands

Command	Description
show running-config interface	Displays the contents of the currently running configuration file.

platform punt-keepalive

To enable the Punt-Keepalive feature and monitor the status of the punt path between the forwarding processor (FP) and the route processor (RP), use the **platform punt-keepalive** command in the global configuration mode. To disable the Punt-Keepalive feature, use the **no** form of this command.

platform punt-keepalive {**disable-kernel-core** | **settings** {**fatal-count** *fatal-count* | **transmit-interval** *transmit-interval* | **warning-count** *warning-count*}}

no platform punt-keepalive

Syntax Description

disable-kernel-core	Disables Linux kernel crash generation and IOS Daemon (IOSD) crash generation.
settings	Specifies the keepalive parameters.
fatal-count *fatal-count*	Specifies the upper limit of consecutive keepalive warnings for triggering system failures. The range is from 15 to 60. Linux kernel crash generation and IOSD crash generation occur when the fatal count reaches the upper limit.
transmit-interval *transmit-interval*	Specifies the keepalive transmit interval, in seconds. The range is from 2 to 30. The default is 2.
warning-count *warning-count*	Specifies the upper limit of consecutive keepalive message failures for reporting warnings. The range is from 10 to 60. Linux kernel crash generation and IOSD crash generation occur when the warnings reach the upper limit.

Command Default

The Punt-Keepalive feature is enabled, and the Kernel core crash and IOSD crash generation are enabled.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Release 3.5S	This command was introduced.

Usage Guidelines

The **platform punt-keepalive** command is available only if all the following conditions are met:

- Device is in an active state.
- FP is present and is online.
- System reload is not in progress.

The punt-keepalive process checks the status of the device and the FP every 30 seconds. However, when the status for the device changes from standby to active, or when the FP goes online, the device waits for another 30 seconds before sending the first keepalive message. Disabling the Linux kernel crash generation and IOS Daemon (IOSD) crash generation allows the system to settle down after the occurrence of critical events.

IOSD or Kernel driver code can cause a keepalive failure; a keepalive failure can force IOSD crash generation and Linux kernel crash generation. The crash generation type depends on the chassis and the operating mode. The following table describes the relationship between chassis, operation mode, and type of crash generation.

Table 3: Relationship Between Chassis, Operation Mode, and Type of Crash Generation

Chassis	Operation Mode	Redundancy Status	Type of Crash Generation
Cisco ASR 1002 Cisco ASR 1002-F	Single IOSD	-	IOSD core Kernel core
Cisco ASR 1001 ASR 1004	Dual IOSD	Not Hot	IOSD core Kernel core
IOSD core Kernel core	Dual IOSD	Hot	IOSD core
Cisco ASR 1006 Cisco ASR 1013	Single or Dual RP	Any	IOSD core Kernel core

Kernel core crash generation takes approximately five minutes. Disable kernel core crash generation for a faster reboot of the system.

Examples

The following example shows how to disable kernel core crash generation and IOSD crash generation by using the **platform punt-keepalive** command:

```
Device(config)# platform punt-keepalive disable-kernel-core
```

Related Commands

Command	Description
show platform software infrastructure punt-keepalive	Displays information about **platform punt-keepalive** command settings.

platform punt-arp-unicast cpu-queue-host

To punt ARP unicast packets through the Routing protocol queue, when packets are forwarded between the forwarding processor (FP) and the route processor (RP), use the **platform punt-arp-unicast cpu-queue-host** command in the global configuration mode. To punt ARP unicast packets through the Broadcast queue, use the **no** form of this command.

Note This command is supported on Cisco IOS XE ASR 920 platforms.

platform punt-arp-unicast cpu-queue-host

no platform punt-arp-unicast cpu-queue-host

Command Default

The platform punt-arp-unicast feature is not enabled by default.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Release 17.10.1	This command was modified.

platform scp retry interval

To enable Switch-Module Configuration Protocol (SCP) fast retry and set the fast-retry interval, use the **platformscpretryinterval** command in global configuration mode. To disable SCP fast retry, use the **no** form of this command.

platform scp retry interval *timeout-value*
no platform scp retry interval

Syntax Description

timeout-value	Fast retry interval; valid values are from 200 to 2000 milliseconds.

Command Default

2000 milliseconds

Command Modes

Global configuration

Command History

Release	Modification
12.2(18)SXD	Support for this command was introduced on the Supervisor Engine 720.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

Note Use this command under the direction of the Cisco TAC only.

Examples

This example shows how to enable SCP fast retry and set the fast-retry interval:

```
Router(config)# platform scp retry interval 600
Router(config)#
```

platform smart-sfp

To configure the Gigabit Ethernet or TenGig Ethernet as VCoP smart SFP on OC3 or OC12 or DS3 mode, use the **platform smart-sfp interface** command in SONET/PDH configuration mode. To remove the VCoP smart SFP, use the **no** form of this command.

platform smart-sfp interface gig/tengig*slot/bay/port* **type***OC3/OC12/DS3*

no platform smart-sfp

Syntax Description

Syntax Description

platform	Specifies a platform keyword.
smart sfp	Specifies a smart sfp keyword. SFP stands for Small Form-Factor Pluggable.
interface	Specifies a interface keyword.
gig/tengig	Specifies the Gigabit Ethernet or TenGig Ethernet port where VCoP is inserted.
slot	Slot number of the controller. A forward slash mark (/) is required between the slot argument and the bay argument.
bay	Bay number of the controller. A forward slash mark (/) is required.
port	Port number of the controller. A forward slash mark (/) is required between the bay argument and the port argument.
type	Type of the interface to be configured. The interface type can be OC3/OC12/ DS3.

Command Modes

Global configuration

Command History

Release	Modification
XE 3.18SP	Support for this command was introduced on the Cisco NCS 4200 Series.
XE Everest 16.5.1	This command was introduced to support DS3 mode of VCoP Smart SFP for Cisco NCS 4200 Series and Cisco ASR 920 Routers.

Usage Guidelines

This command is used to identify the VCoP OC-n/DS3 smart SFP inserted in the Cisco NCS 4200 Series. This command is used to configure VCoP OC-n smart SFP type i.e. OC3 or OC12 and DS3 mode. Before executing this command for a particular port, the configuration on that port must be deleted or set as default.

This command sets the Gig port as the smart SFP port for configuring the CEP for the given port number.

Examples

The following example shows how to configure VCoP smart SFP on Gig and TenGig ports.

Configruing VCoP smart SFP on OC3 mode

For Gigabit port:

```
Router(config)# configure terminal
Router(config)# platform smart-sfp interface GigabitEthernet 0/0/8 type OC-3
```

For TenGig port:

```
Router(config)# configure terminal
Router(config)# platform smart-sfp interface TenGig 0/0/8 type OC-3
```

Configruing VCoP smart SFP on OC12 mode

For Gigabit port:

```
Router(config)# configure terminal
Router(config)# platform smart-sfp interface GigabitEthernet 0/0/8 type OC-12
```

For TenGig port:

```
Router(config)# configure terminal
Router(config)# platform smart-sfp interface TenGig 0/0/8 type OC-12
```

Configruing VCoP smart SFP on T3 mode

For Gigabit port:

```
Router(config)# configure terminal
Router(config)# platform smart-sfp interface GigabitEthernet 0/0/8 type ds3
```

For TenGig port:

```
Router(config)# configure terminal
Router(config)# platform smart-sfp interface TenGig 0/0/8 type ds3
```

Related Commands

Command	Description
show cem circuit	Displays the circuit emulation (CEM) statistics for the configured CEM circuits.
show controller	Displays SONET/T3 controller configuration.

platform time-source

To initiate Time of Day (ToD) synchronization on a line card, use the **platformtime-source** command in global configuration mode. To disable the platform time-source, use the **no** form of this command.

platform time-source {**ntp** | **ptp**}
no platform time-source

Syntax Description

ntp	Configures Network Time Protocol (NTP) clock source
ptp	Configures Precision Time Protocol (PTP) clock source

Command Default

The **platformtime-source** command is not enabled.

Command Modes

Global configuration

Command History

Release	Modification
15.1(2)S	This command was introduced on the Cisco 7600 routers.
Cisco IOS XE Release 3.12	This command is integrated on the Cisco ASR 900 Series Routers. The **ptp** keyword is not supported on the Cisco ASR 900 Series Routers.

Usage Guidelines

Cisco 7600 Router

Either the 2-Port Gigabit Synchronous Ethernet SPA (PTP) or NTP module on the Route Processor is used to initiate the ToD synchroniztion. The NTP ToD information is converted into PTP format and then synchronized to all the ES+ Linecards.

Cisco ASR 900 Series Routers

This command is used to enable or disable NTP clock (Time of Day) synchronization on the ethernet ports. The ports will use NTP ToD value to timestamp Y.1731 DM packets.

Example

This example shows how to configure platform time-source on the Cisco ASR 900 Series Router.

```
Router (config)# platform time-source ntp
```

Examples

This example shows how to configure the platform time-source on the Cisco 7600 Router.

```
Router (config)#platform time-source ptp 1 master top 6/0/2 slave lo0
or
Router (config)#platform time-source ntp
```

Related Commands

Command	Description
show platform time-source	This command displays the configuration details of the platform time-source.

platform trace boottime process forwarding-manager module interfaces

To enable Forwarding Manager Route Processor and Embedded Service Processor trace messages for the RP forwarding manager process during bootup, use the **platformtraceboottimeprocessforwarding-managermoduleinterfaces**command in the Global configuration mode. To disable debug messages, use the **no** form of this command.

platform trace boottime slot *slot* **bay** *bay* **process forwarding-manager module interfaces level** *level*
no platform trace boottime slot *slot* **bay** *bay* **process forwarding-manager module interfaces**

Syntax Description

slot	Shared Port Adapter (SPA) Interprocessor, Embedded Service Processor or Route Processor slot. Valid options are: • *R0* --Route Processor slot 0 • *R1* --Route Processor slot 1
bay	Chassis bay to be configured. Valid options are: • *0* • *1*
level *level*	Selects the trace level. The trace level determines the amount of information that is to be stored about a module in the trace buffer or file. Valid options are: • **max** --Provides the maximum possible message. • **notice messages** --Provides notice messages.

Command Default

The default tracing level for every module on the Cisco ASR 1000 Series Routers is Notice.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Release 3.2S	This command was introduced on the Cisco ASR 1000 Routers.

Usage Guidelines

Trace-level settings are leveled that is every setting contains all the messages from the lower setting plus the messages from its own setting. For instance, setting the trace level to 3 (error) ensures that the trace file contains all the output for the 0 (emergencies), 1 (alerts), 2 (critical), and 3 (error) settings. Setting the trace level to 4 (warning) ensures that all the trace output for a specific module is included in that trace file.

All trace levels cannot be configured by users. Specifically, the alert, critical, and notice tracing levels cannot be set by users. To trace these messages, set the trace level to a higher level, which collects these messages.

When setting the trace levels, it is also important to remember that the setting is not done in a configuration mode. As a result of this, trace level settings are returned to their defaults after every router reload.



Caution Setting tracing of a module to the debug level or higher can have a negative performance impact. Setting tracing to the debug level or higher should be done with discretion.



Caution Setting a large number of modules to high tracing levels can severely degrade performance. If a high level of tracing is needed in a specific context, it is almost always preferable to set a single module on a higher tracing level rather than setting multiple modules to high tracing levels.

Examples

In the following example, the trace level for the forwarding processor module in the Forwarding Manager of the ESP processor in slot R0 is set to the informational tracing level (max):

```
Router(config)# platform trace boottime slot R0 bay 1 process forwarding-manager
forwarding-manager level max
```

Related Commands

Command	Description
show platform software trace level	Displays trace levels for specified modules.
show platform software trace message	Displays trace messages.

pm fec threshold

To configure performance monitoring thresholds on the FEC layer, use the **pmfecthreshold**command in DWDM configuration mode. To disable the performance monitoring threshold, use the **no** form of this command.

pm {**15-min** | **24-hour**} **fec threshold** {**ec-bits** | **uc-words**} *threshold*
nopm {**15-min** | **24-hour**} **fec threshold** {**ec-bits** | **uc-words**} *threshold*

Syntax Description

15-min	Configures the performance monitoring thresholds for 15-minute intervals.
24-hour	Configures performance monitoring thresholds for 24-hour intervals.
ec-bits	Bit errors corrected (BIEC). Indicates the number of bit errors corrected in the DWDM trunk line during the performance monitoring time interval.
uc-words	Uncorrectable Words. Indicates the number of uncorrectable words detected in the DWDM trunk line during the performance monitoring time interval.
threshold	Threshold for the performance monitoring parameter.

Command Default

No threshold is configured.

Command Modes

DWDM configuration.

Command History

Release	Modification
15.1(3)S	This command was introduced on the Cisco 7600 series routers.

Examples

The following example shows how to configure an FEC layer performance monitoring threshold for uncorrectable words:

```
Router(config)# controller dwdm 0/0
Router(config-controller)# pm 15-min fec threshold uc-words 900 enable
```

Related Commands

Command	Description
show controller dwdm pm fec	Displays performance measurement information for the FEC layer.

pm optics report

To enable threshold crossing alert (TCA) generation on the optics layer, use the **pmopticsreport**command in DWDM configuration mode. To disable TCA reporting, use the **no** form of this command.

pm {**15-min** | **24-hour**} **optics report** {**lbc** | **opr** | **opt**} {**max-tca** | **min-tca**} **enable**
nopm {**15-min** | **24-hour**} **optics report** {**lbc** | **opr** | **opt**} {**max-tca** | **min-tca**} **enable**

Syntax Description

15-min	Configures TCA generation for 15-minute intervals.
24-hour	Configures TCA generation for 24-hour intervals.
lbc	Laser bias current.
opr	Optical power on the unidirectional port.
opt	Transmit optical power in dBm.
max-tca	Indicates that the maximum value of the parameter is compared against the threshold to determine if a TCA should be generated.
min-tca	Indicates that the minimum value of the parameter is compared against the threshold to determine if a TCA should be generated.
enable	Enables TCA generation for the specified parameter on the DWDM controller.

Command Default

TCA reporting is not enabled.

Command Modes

DWDM configuration.

Command History

Release	Modification
15.1(3)S	This command was introduced on the Cisco 7600 series routers.

Examples

The following example shows how to enable TCA reporting on the optics layer reporting for the maximum OPT:

```
Router(config)# controller dwdm 0/0
Router(config-controller)# pm 15-min optics report opt max-tca enable
```

Related Commands

Command	Description
show controller dwdm pm optics	Displays performance measurement information for the optics layer.

pm otn report

To enable threshold crossing alert (TCA) generation on the optical transport network (OTN) layer, use the **pmotnreport**command in DWDM configuration mode. To disable TCA reporting, use the **no** form of this command.

pm {**15-min** | **24-hour**} **otn report** *otn-parameter* **enable**
nopm {**15-min** | **24-hour**} **otn report** *otn-parameter* **enable**

Syntax Description

15-min	Configures TCA generation for 15-minute intervals.
24-hour	Configures TCA generation for 24-hour intervals.
otn-parameter	Specific parameter for which to configure the threshold. OTN parameters can be as follows: • **bbe-pm-fe** --Far-end path monitoring background block errors (BBE-PM). Indicates the number of background block errors recorded in the optical transport network (OTN) path during the performance monitoring time interval. • **bbe-pm-ne** --Near-end path monitoring background block errors (BBE-PM). • **bbe-sm-fe** --Far-end section monitoring background block errors (BBE-SM). Indicates the number of background block errors recorded in the OTN section during the performance monitoring time interval. • **bbe-sm-ne** --Near-end section monitoring background block errors (BBE-SM). • **bber-pm-fe** --Far-end path monitoring background block errors ratio (BBER-PM). Indicates the background block errors ratio recorded in the OTN path during the performance monitoring time interval. • **bber-pm-ne** --Near-end path monitoring background block errors ratio (BBER-PM). • **bber-sm-fe** --Far-end section monitoring background block errors ratio (BBER-SM). Indicates the background block errors ratio recorded in the OTN section during the performance monitoring time interval. • **bber-sm-ne** --Near-end section monitoring background block errors ratio (BBER-SM) • **es-pm-fe** --Far-end path monitoring errored seconds (ES-PM). Indicates the errored seconds recorded in the OTN path during the performance monitoring time interval. • **es-pm-ne** --Near-end path monitoring errored seconds (ES-PM). • **es-sm-fe** --Far-end section monitoring errored seconds (ES-SM). Indicates the errored seconds recorded in the OTN section during the performance monitoring time interval. • **es-sm-ne** --Near-end section monitoring errored seconds (ES-SM). • **esr-pm-fe** --Far-end path monitoring errored seconds ratio (ESR-PM). Indicates the errored seconds ratio recorded in the OTN path during the performance monitoring time interval.

	• **esr-pm-ne** --Near-end path monitoring errored seconds ratio (ESR-PM). • **esr-sm-fe** --Far-end section monitoring errored seconds ratio (ESR-SM). Indicates the errored seconds ratio recorded in the OTN section during the performance monitoring time interval. • **esr-sm-ne** --Near-end section monitoring errored seconds ratio (ESR-SM). • **fc-pm-fe** --Far-end path monitoring failure counts (FC-PM). Indicates the failure counts recorded in the OTN path during the performance monitoring time interval. • **fc-pm-ne** --Near-end path monitoring failure counts (FC-PM). • **fc-sm-fe** --Far-end section monitoring failure counts (FC-SM). Indicates the failure counts recorded in the OTN section during the performance monitoring time interval. • **fc-sm-ne** --Near-end section monitoring failure counts (FC-SM). • **ses-pm-fe** --Far-end path monitoring severely errored seconds (SES-PM). Indicates the severely errored seconds recorded in the OTN path during the performance monitoring time interval. • **ses-pm-ne** --Far-end path monitoring severely errored seconds (SES-PM). • **ses-sm-fe** --Far-end section monitoring severely errored seconds (SES-SM). Indicates the severely errored seconds recorded in the OTN section during the performance monitoring time interval. • **ses-sm-ne** --Near-end section monitoring severely errored seconds (SES-SM). • **sesr-pm-fe** --Far-end path monitoring severely errored seconds ratio (SESR-PM). Indicates the severely errored seconds ratio recorded in the OTN path during the performance monitoring time interval. • **sesr-pm-ne** --Near-end path monitoring severely errored seconds ratio (SESR-PM). • **sesr-sm-fe** --Far-end section monitoring severely errored seconds ratio (SESR-SM). Indicates the severely errored seconds ratio recorded in the OTN section during the performance monitoring time interval. • **sesr-sm-ne** --Near-end section monitoring severely errored seconds ratio (SESR-SM). • **uas-pm-fe** --Far-end path monitoring unavailable seconds (UAS-PM). Indicates the unavailable seconds recorded in the OTN path during the performance monitoring time interval. • **uas-pm-ne** --Near-end path monitoring unavailable seconds (UAS-PM). • **uas-sm-fe** --Far-end section monitoring unavailable seconds (UAS-SM). Indicates the unavailable seconds recorded in the OTN section during the performance monitoring time interval. • **uas-sm-ne** --Near-end section monitoring unavailable seconds (UAS-SM).
enable	Enables TCA generation for the specified parameter on the DWDM controller.

Command Default TCA generation is not enabled.

Command Modes

DWDM configuration.

Command History

Release	Modification
15.1(3)S	This command was introduced on the Cisco 7600 series routers.

Examples

The following example shows how to enable TCA generation on the OTN layer reporting for the path monitoring errored seconds ratio (ESR-PM):

```
Router(config)# controller dwdm 0/0
Router(config-controller)# pm 15-min otn report esr-pm-fe enable
```

Related Commands

Command	Description
show controller dwdm pm otn	Displays performance measurement information for the OTN layer.

pm optics threshold

To configure performance monitoring thresholds on the optics layer, use the **pmopticsthreshold**command in DWDM configuration mode. To disable the performance monitoring threshold, use the **no** form of this command.

pm {**15-min** | **24-hour**} **optics threshold** {**lbc** | **opr** | **opt**} {**max** | **min**} *threshold*
nopm {**15-min** | **24-hour**} **optics threshold** {**lbc** | **opr** | **opt**} {**max** | **min**} *threshold*

Syntax Description

15-min	Configures performance monitoring thresholds for 15-minute intervals.
24-hour	Configures performance monitoring thresholds for 24-hour intervals.
lbc	Laser bias current.
opr	Optical power on the unidirectional port.
opt	Transmits optical power in dBm.
max	Indicates that the *threshold* is for the maximum value of the parameter.
min	Indicates that the *threshold* is for the minimum value of the parameter.
threshold	Threshold for the performance monitoring parameter.

Command Default

No thresholds are configured.

Command Modes

DWDM configuration.

Command History

Release	Modification
15.1(3)S	This command was introduced on the Cisco 7600 series routers.

Examples

The following example shows how to configure an optics layer performance monitoring threshold for maximum OPT:

```
Router(config)# controller dwdm 0/0
Router(config-controller)# pm 15-min optics threshold opt max 700
```

Related Commands

Command	Description
show controller dwdm pm optics	Displays performance measurement information for the optics layer.

pm otn threshold

To configure performance monitoring thresholds on the optical transport network (OTN) layer, use the **pmotnthreshold**command in DWDM configuration mode. To disable TCA reporting, use the **no** form of this command.

pm {**15-min** | **24-hour**} **otn threshold** *otn-parameter threshold*
nopm {**15-min** | **24-hour**} **otn threshold** *otn-parameter threshold*

Syntax Description

15-min	Configures performance monitoring thresholds for 15-minute intervals.
24-hour	Configures performance monitoring thresholds for 24-hour intervals.
otn-parameter	Specific parameter for which to configure the threshold. OTN parameters can be as described in the **pmotnreport** command.
threshold	Threshold for the performance monitoring parameter.

Command Default

No thresholds are configured.

Command Modes

DWDM configuration.

Command History

Release	Modification
15.1(3)S	This command was introduced on the Cisco 7600 series routers.

Examples

The following example shows how to configure an OTN layer performance monitoring threshold for path monitoring errored seconds ratio (ESR-PM):

```
Router(config)# controller dwdm 0/0
Router(config-controller)# pm 15-min otn threshold esr-pm-ne 800
```

Related Commands

Command	Description
show controller dwdm pm otn	Displays performance measurement information for the OTN layer.

port (interface)

To enable an interface on a PA-4R-DTR port adapter to operate as a concentrator port, use the **port**command in interface configuration mode. To restore the default station mode, use the **no** form of this command.

port
no port

Syntax Description

This command has no arguments or keywords.

Command Default

Station mode

Command Modes

Interface configuration

Command History

Release	Modification
11.3(3)T	This command was introduced.

Usage Guidelines

By default, the interfaces of the PA-4R-DTR operate as Token Ring stations. Station mode is the typical operating mode. Use this command to enable an interface to operate as a concentrator port.

Examples

The following example configures the PA-4R-DTR ports to operate in concentrator mode on a Cisco 7000 series router:

```
Router(config)# interface tokenring 3/0/0
Router(config-if)# port
```

port access-map

To create a port access map or enter port access-map command mode, use the **portaccess-map** command in global configuration mode. To remove a mapping sequence or the entire map, use the **no** form of this command.

port access-map *name* [*seq#*]
no port access-map *name* [*seq#*]

Syntax Description

name	Port access-map tag.
seq#	(Optional) Map sequence number; valid values are 0 to 65535.

Command Default

This command has no default settings.

Command Modes

Global configuration

Command History

Release	Modification
12.2(14)SX	Support for this command was introduced on the Supervisor Engine 720.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

This command is not supported on Cisco 7600 series routers that are configured with a Supervisor Engine 2.

If you enter the sequence number of an existing map sequence, you enter port access-map mode. If you do not specify a sequence number, a number is automatically assigned. You can enter one match clause and one action clause per map sequence.

If you enter the **noportaccess-mapname** [*seq#*] command without entering a sequence number, the whole map is removed.

Once you enter port access-map mode, the following commands are available:

- **action** -- Specifies the packet action clause; see the **action** command section.
- **default** -- Sets a command to its defaults.
- **end** -- Exits from configuration mode.
- **exit** -- Exits from the port access-map configuration mode.
- **match** -- Specifies the match clause; see the **match** command section.
- **no** -- Negates a command or sets its defaults.

Examples

This example shows how to enter port access-map mode:

```
Router(config)# port access-map ted
Router(config-port-map)#
```

Related Commands

Command	Description
action	Sets the packet action clause.
match	Specifies the match clause by selecting one or more ACLs for a VLAN access-map sequence.

port-channel hash-distribution

To set the hash distribution algorithm method, use the port-channel hash-distribution command in global configuration mode. To return to the default settings, use the **no** or **default** form of this command.

port-channel hash-distribution {**adaptive** | **fixed**}
{**no** | **default**} **port-channel hash-distribution**

Syntax Description

adaptive	Specifies selective distribution of the bundle select register among the port-channel members.
fixed	Specifies fixed distribution of the bundle select register among the port-channel members.
default	Specifies the default setting.

Command Default

The hash distribution algorithm method is set to **fixed.**

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(33)SXH	This command was introduced.
12.2(33)SRC	This command was integrated into Cisco IOS Release 12.2(33)SRC.

Usage Guidelines

The EtherChannel load distribution algorithm uses the bundle select register in the port ASIC to determine the port for each outgoing packet. When you use the **adaptive** algorithm, it does not require the bundle select register to be changed for existing member ports. When you use the **fixed** algorithm and you either add or delete a port from the EtherChannel, the switch updates the bundle select register for each port in the EtherChannel. This update causes a short outage on each port.



Note When you change the algorithm, the change is applied at the next member link event. Example events include link down, up, addition, deletion, no shutdown, and shutdown. When you enter the command to change the algorithm, the command console issues a warning that the command does not take effect until the next member link event.

Examples

The following example shows how to set the hash distribution algorithm method to adaptive:

```
Router(config)# port-channel hash-distribution adaptive
```

port-channel load-balance

To set the load distribution method among the ports in a bundle, use the **port-channelload-balance** command in global configuration mode. To reset the load distribution to the default settings, use the **no** form of this command.

port-channel load-balance *method* **module** *slot*
no port-channel load-balance

Syntax Description

method	Load distribution method; see the "Usage Guidelines" section for a list of valid values.
module	Specifies the module on which the load-distribution method is set. This keyword is supported only on DFC systems.
slot	Number of the slot in the module.

Command Default

The default**method** is **src-dst-ip**.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(14)SX	This command was introduced on the Supervisor Engine 720.
12.2(17d)SXB	This command was modified to support the Supervisor Engine 2.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was modified. The following keywords were added: **dst-mixed-ip-port**,**src-dst-mixed-ip-port**,**src-mixed-ip-port**,and**excludevlan**. • These keywords are supported on systems that are in PFC3C or PFC3CXL mode (PFC3C or PFC3CXL with no DFC3A or DFC3B/BXL) only. • The **excludevlan**keyword is added only for IP-related load balance options.

Usage Guidelines

Valid *method* values are as follows:

- **dst-ip** --Loads distribution on the destination IP address. Option to exclude VLAN in the distribution is provided using the **excludevlan**keyword along with this method.
- **dst-mac** --Loads distribution on the destination MAC address.
- **dst-mixed-ip-port** --Loads distribution on the destination IP address and TCP or User Datagram Protocol (UDP) port. Option to exclude VLAN in the distribution is provided using the **excludevlan**keyword along with this method.
- **dst-port** --Loads distribution on the destination port.
- **src-dst-ip** --Loads distribution on the source transfer or XOR-destination IP address. Option to exclude VLAN in the distribution is provided using the **excludevlan**keyword along with this method.

- **src-dst-mac** --Loads distribution on the source XOR-destination MAC address.
- **src-dst-mixed-ip-port** --Loads distribution on the source XOR-destination IP address and the TCP or UDP port. Option to exclude VLAN in the distribution is provided using the **excludedvlan**keyword along with this method.
- **src-dst-port** --Loads distribution on the source XOR-destination port.
- **src-ip** --Loads distribution on the source IP address. Option to exclude VLAN in the distribution is provided using the **excludedvlan**keyword along with this method.
- **src-mac** --Loads distribution on the source MAC address.
- **src-mixed-ip-port** --Loads distribution on the source IP address and the TCP or UDP port. Option to exclude VLAN in the distribution is provided using the **excludedvlan**keyword along with this method.
- **src-port** --Loads distribution on the source port.

The **port-channelload-balance***method***module***slot* command is supported on DFC systems only.

The **port-channelper-moduleload-balance** command allows you to enable or disable port-channel load-balancing on a per-module basis. You can enter the **port-channelload-balance***method***module***slot* command to specify the load-balancing method on a specific module after you have entered the **port-channelper-moduleload-balance**command.

The following keywords are supported on systems that are in PFC3C or PFC3CXL mode (PFC3C or PFC3CXL with no DFC3A or DFC3B/BXL) only:

- **dst-mixed-ip-port**
- **src-dst-mixed-ip-port**
- **src-mixed-ip-port**

Note If you change the load-balancing method, EtherChannel ports on DFC-equipped switching modules or an active supervisor engine in a dual supervisor engine configuration will flap.

Examples

The following example shows how to set the load-distribution method to **dst-ip**:

```
Router(config)#
port-channel load-balance dst-ip
```

The following example shows how to set the load-distribution method on a specific module:

```
Router(config)#
port-channel load-balance dst-ip module 2
```

The following example shows how to set the load-distribution method excluding the VLAN option:

```
Router(config)#
port-channel load-balance dst-ip exclude vlan
```

Related Commands

Command	Description
interface port-channel	Creates a port-channel virtual interface and enters interface configuration mode.
port-channel load-balance mpls	Sets the load distribution method among the ports in the bundle for MPLS packets.
show etherchannel	Displays the EtherChannel information for a channel.

port-channel load-balance (interface)

To configure a member link for load balancing, a default service instance weight, or weighted load balancing on port-channel member links, use the **port-channel load-balance** command in interface configuration mode. To cause the default weight to revert to 1 and to disable weighted load balancing, use the **no** form of this command.

port-channel load-balance {**link** *link-id* | **weighted** {**default weight** *weight* | **link** {**all***link-id*} | **rebalance** {**disable***weight*}}}
no port-channel load-balance {**link** *link-id* | **weighted** {**default weight** | **link** | **rebalance**}}

Syntax Description

link	Configures a member link for egress load balancing.
link-id	Integer from 1 to 16 that identifies the member link. • When used with the **weighted** keyword, the *link-id* is a comma-delimited list of member link IDs to use for weighted load balancing.
weighted	Configures weighted load balancing on the port channel.
default weight	Configures a default weight for a service instance.
weight	Integer from 1 to 10000 that is the weight value. The default is 1. • When used with the **rebalance** keyword, this value is the threshold weight used to trigger automatic rebalancing. The default is 4.
all	Configures load balancing across all active member links.
rebalance	Sets or disables the automatic rebalance threshold.
disable	Disables automatic rebalancing.

Command Default

Service instance weight and weighted load balancing are not configured.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
15.0(1)S	This command was introduced.

Usage Guidelines

When weighted load balancing enabled, the weight configured using this command is inherited by all service instances on the port channel that have not been specifically configured with a weight.

Configuring a default weight is optional; the default weight value is 1.

Use of the **weighted**and **link** keywords is required to enable weighted load balancing on a port channel. When the **all** keyword is configured, traffic is distributed across all active member links in the port channel. When one or more member links is specified, traffic is distributed across only those member links. To allow for out-of-order configuration, link IDs not yet assigned to member links may be specified. Issuing this command

with the **weighted** and **link** keywords more than once under the same port-channel interface results in overwriting the command settings previously configured.

If this command is configured with a list of link IDs and the member link corresponding to one of those link IDs is later configured with a different ID, a warning is displayed on the console that notifies the user that the action will affect the current load-balancing activity.

When the **disable** keyword is configured, automatic rebalancing is not performed and the operator must manually invoke rebalancing by issuing the **port-channel load-balance weighted rebalance**command in privileged EXEC mode.

When the **disable** keyword is not configured, either the configured or a default weight is used to automatically rebalance service instances. Automatic rebalancing occurs when the average absolute deviation (AAD) of the current distribution exceeds the configured threshold and when the resulting AAD of the rebalanced distribution is less than the current AAD. If automatic rebalancing does not result in a lower AAD, the rebalancing is not done, even if the current AAD exceeds the threshold.

The AAD calculation is (1/*n*)*Sum(|w(*i*) - m|) for all *n* member links where:

n = number of member links

m = mean of member link weights (sum of all Ethernet service instance weights divided by *n*)

w (*i*) = sum of Ethernet service instance weights on member link *i*

Two conditions cause the **port-channel load-balance**command to fail:

- An invalid weight is configured.
- An invalid link ID is provided.

Examples

The following example shows how to configure port-channel load balancing for all port-channel member links:

```
Router(config)# interface port-channel1
Router(config-if)# port-channel load-balance weighted link all
```

port-channel load-balance mpls

To set the load-distribution method among the ports in the bundle for Multiprotocol Label Switching (MPLS) packets, use the **port-channel load-balance mpls**command in global configuration mode. To reset the load distribution to the default settings, use the **no** form of this command.

port-channel load-balance mpls {**label** | **label-ip**}
no port-channel load-balance mpls

Syntax Description

label	Specifies using the MPLS label to distribute packets; see the "Usage Guidelines" section for additional information.
label-ip	Specifies using the MPLS label or the IP address to distribute packets; see the "Usage Guidelines" section for additional information.

Command Default

label-ip

Command Modes

Global configuration

Command History

Release	Modification
12.2(14)SX	Support for this command was introduced on the Supervisor Engine 720.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

This command is not supported on Cisco 7600 series routers that are configured with a Supervisor Engine 2.

If you select **label**, these guidelines apply:

- With only one MPLS label, the last MPLS label is used.
- With two or more MPLS labels, the last two labels (up to the fifth label) are used.

If you select **label-ip**, these guidelines apply:

- With IPv4 and three or fewer labels, the source IP address XOR-destination IP address is used to distribute packets.
- With four or more labels, the last two labels (up to the fifth label) are used.
- With non-IPv4 packets, the distribution method is the same as the **label** method.

Examples

This example shows how to set the load-distribution method to **label-ip**:

```
Router(config)#
port-channel load-balance mpls label-ip
Router(config)#
```

Related Commands

Command	Description
interface port-channel	Creates a port-channel virtual interface and enters interface configuration mode.
show etherchannel	Displays the EtherChannel information for a channel.

port-channel load-balance weighted rebalance

To perform a rebalancing of all port-channel interfaces configured with weighted load balancing, use the **port-channel load-balance weighted rebalance** command in privileged EXEC mode.

port-channel load-balance weighted rebalance [**interface port-channel** *number*]

Syntax Description

interface	(Optional) Specifies a port channel enabled for weighted load balancing.
port-channel	(Optional) Specifies an Ethernet channel of interfaces.
number	(Optional) Integer from 1 to 564 that identifies the port-channel interface.

Command Default

Load rebalancing is not performed.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
15.0(1)S	This command was introduced.

Usage Guidelines

If a port-channel interface is specified, only that interface is rebalanced; otherwise all port channels with weighted load balancing enabled are rebalanced.

This command may be used when automatic rebalancing is disabled via the **port-channel load-balance weighted rebalance disable** command or when a rebalancing of service instances is desired prior to reaching the automatic rebalance threshold.

If the specified interface is not a port channel enabled for weighted load balancing, the **port-channel load-balance weighted rebalance**command has no effect on load balancing on that interface.

Examples

The following example shows how to force a rebalancing of service instances, based on their assigned weights, for all port channels with weighted load balancing enabled:

```
Router# port-channel load-balance weighted rebalance
```

Related Commands

Command	Description
port-channel load-balance (interface)	Configures a member link for load balancing, a default service instance weight, or weighted load balancing on port-channel member links.

port-channel load-balancing vlan-manual

To apply the VLAN-manual load-balancing method globally to all Gigabit EtherChannel (GEC) interfaces, use the **port-channelload-balancingvlan-manual**command in global configuration mode. To reset to the default, use the **no** form of this command.

port-channel load-balancing vlan-manual
no port-channel load-balancing

Syntax Description

This command has no arguments or keywords.

Command Default

Flow-based load balancing is enabled.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Release 2.1	This command was introduced.
Cisco IOS XE Release 2.5	This command was modified. The default was changed from no load balancing is enabled to flow-based load balancing.

Usage Guidelines

The **port-channelload-balancingvlan-manual** command applies the VLAN-manual load-balancing method globally to all port channels on the router. If you do not use this command to explicitly set the global load-balancing method to VLAN-manual, the load-balancing method is set to flow-based.

The load-balancing method enabled on a port channel with the **load-balancing**command takes precedence over this command.

Load balancing uses the concept of buckets to map traffic flows to the member links of a port channel. The different traffic flows are mapped to the buckets and each bucket has one active member link associated with it. All flows that are mapped to a bucket use the member link associated with that bucket.

There are two methods of load balancing on a GEC interface:

- VLAN-manual--All packets forwarded over the same VLAN subinterface are considered part of the same flow and are mapped to the member link specified in the configuration.
- Flow-based--Traffic flows are mapped to different member links based on the packet header.

Examples

This example shows how to set the load-balancing method to VLAN-manual:

```
Router(config)# port-channel
load-balancing vlan-manual
```

Related Commands

Command	Description
interface port-channel	Creates a port-channel virtual interface.
load-balancing	Applies a load-balancing method to a GEC interface.

Command	Description
show interfaces port-channel etherchannel	Displays the load-balancing bucket distribution currently in use for a GEC interface.
show etherchannel load-balancing	Displays the load-balancing method applied to GEC interfaces.

port-channel load-defer

To configure the port load share deferral interval for all port channels, use the **port-channelload-defer** command in global configuration mode. To reset the port defer interval to the default setting, use the **no** form of this command.

port-channel load-defer *seconds*
no port-channel load-defer *seconds*

Syntax Description

seconds	Sets the time interval in seconds by which load sharing will be deferred on the switch. Valid range is from 1 to 1800 seconds. The default deferal interval is 120 seconds

Command Default

The port defer interval is 120 seconds.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(33)SXH	This command was introduced.
12.2(50)SY	This command was introduced. Added the *seconds* variable for use in Cisco IOS Release 12.2(50)SY.

Usage Guidelines

To reduce data loss following a stateful switchover (SSO), port load share deferral can be enabled by entering the **port-channelportload-defer** command on a port channel of a switch that is connected by a multichassis EtherChannel (MEC) to a virtual switching system (VSS). Port load share deferral temporarily prevents the switch from forwarding data traffic to MEC member ports on a failed chassis of the VSS while the VSS recovers from the SSO.

The load share deferral interval is determined by a single global timer configurable by the **port-channelload-defer** command. After an SSO switchover, a period of several seconds to several minutes can be required for the reinitialization of line cards and the reestablishment of forwarding tables, particularly multicast topologies.

The valid range of *seconds* is 1 to 1800 seconds; the default is 120 seconds.

Examples

This example shows how to set the global port deferral interval to 60 seconds:

```
Router(config)#
port-channel load-defer 60
Router(config)#
```

This example shows how to verify the configuration of the port deferral interval on a port channel:

```
Router# show etherchannel 50 port-channel

                Port-channels in the group:
                ----------------------
Port-channel: Po50    (Primary Aggregator)
------------
Age of the Port-channel   = 0d:00h:22m:20s
```

```
Logical slot/port   = 46/5          Number of ports = 3
HotStandBy port = null
Port state          = Port-channel Ag-Inuse
Protocol            =   LACP
Fast-switchover     = disabled
Load share deferral = enabled   defer period = 60 sec
   time left = 57 sec
Router#
```

Related Commands

Command	Description
interface port-channel	Creates a port channel virtual interface and enters interface configuration mode.
port-channel port load-defer	Enables the port load share deferral feature on a port channel.
show etherchannel	Displays the EtherChannel information for a channel.

port-channel min-links

To specify that a minimum number of bundled ports in an EtherChannel is required before the channel can be active, use the **port-channelmin-links** command in interface configuration mode. To return to the default settings, use the **no** form of this command.

port-channel min-links *min-num*
no port-channel min-links

Syntax Description

min-num	Minimum number of bundled ports in a channel that is required before the channel can be active; valid values are from 2 to 8.

Command Default

min-num is **1**

Command Modes

Interface configuration

Command History

Release	Modification
12.2(18)SXF	Support for this command was introduced on the Supervisor Engine 720.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

This command is supported on LACP (802.3ad) ports only. More than one LACP secondary-port channel can belong to the same channel group. This command is applied to all port channels in the same group.

If fewer links than the specified number are available, the port-channel interface does not become active.

Use the **showrunning-config** command to verify the configuration.

Examples

This example shows how to specify that a minimum number of bundled ports in an EtherChannel is required before the channel can be active:

```
Router(config-if)#
port-channel min-links 3
Router(config-if)#
```

Related Commands

Command	Description
show running-config	Displays the status and configuration of the module or Layer 2 VLAN.

port-channel per-module load-balance

To enable load balance on a per-module basis among the ports in a bundle, use the port-channel per-module load-balance command in global configuration mode. To return to the default settings, use the **no** form of this command.

port-channel per-module load-balance
no port-channel per-module load-balance

Syntax Description

This command has no arguments or keywords.

Command Default

The load balance method is not enabled per module**.**

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(18)ZY	This command was introduced.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.

Usage Guidelines

The **port-channelper-moduleload-balance** command allows you to enable or disable port-channel load balancing on a per-module basis. You can use the **port-channelload-balancemodule**command to specify the load balancing method on a specific module after you have entered the **port-channelper-moduleload-balance** command.

Examples

The following example shows how to enable load balancing on a per-module basis:

```
Router(config)# port-channel per-module load-balance
```

Related Commands

Command	Description
port-channel hash-distribution	Sets the hash distribution algorithm method among the ports in a bundle.
port-channel load-balance	Sets the load balance method among the ports in a bundle.

port-channel port load-defer

To enable the temporary deferral of port load sharing during the connection or reconnection of a port channel, use the **port-channelportload-defer** command in interface configuration mode. To disable the deferral of port load sharing on a port channel, use the **no** form of this command.

port-channel port load-defer
no port-channel port load-defer

Syntax Description

This command has no keywords or arguments.

Command Default

The port load share deferral feature is not enabled on a port channel .

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.2(33)SXH	This command was introduced.
12.2(50)SY	This command was introduced.

Usage Guidelines

To reduce data loss following a stateful switchover (SSO), a port load share deferral can be enabled on a port channel of a switch that is connected by a multichassis EtherChannel (MEC) to a virtual switching system (VSS). The load share deferral interval prevents the switch from forwarding data traffic to MEC member ports on a failed chassis of the VSS while the VSS recovers from the SSO.

When load share deferral is enabled on a port channel, the assignment of a member port's load share is delayed for a period that is configurable globally by the **port-channelload-defer** command. During the deferral period, the load share of a deferred member port is set to 0. In this state, the deferred port is capable of receiving data and control traffic, and of sending control traffic, but the port is prevented from sending data traffic over the MEC to the VSS. Upon expiration of the global deferral timer, the deferred member port exits the deferral state and the port assumes its normal configured load share.

Load share deferral is applied only if at least one other member port of the port channel is currently active with a nonzero load share. If a port enabled for load share deferral is the first member bringing up the EtherChannel, the deferral feature does not apply and the port will forward traffic immediately.

The load share deferral interval is determined by a single global timer configurable from 1 to 1800 seconds by the **port-channelload-defer** command. The default interval is 120 seconds. After an SSO switchover, a period of several seconds to several minutes can be required for the reinitialization of line cards and the reestablishment of forwarding tables, particularly multicast topologies.

Examples

This example shows how to enable the load share deferral feature on port channel 50 of a switch that is an MEC peer to a VSS:

```
Router(config)#
interface port-channel 50
Router(config-if)#
port-channel port load-defer

This will enable the load share deferral feature on this port-channel.
```

```
The port-channel should connect to a Virtual Switch (VSS).
Do you wish to proceed? [yes/no]:
yes
Router(config-if)#
```

This example shows how to verify the state of the port deferral feature on a port channel:

```
Router# show etherchannel 50 port-channel

                Port-channels in the group:
                ----------------------
Port-channel: Po50    (Primary Aggregator)
------------
Age of the Port-channel   = 0d:00h:22m:20s
Logical slot/port   = 46/5          Number of ports = 3
HotStandBy port = null
Port state          = Port-channel Ag-Inuse
Protocol            =   LACP
Fast-switchover     = disabled
Load share deferral = enabled   defer period = 120 sec   time left = 57 sec
Router#
```

Related Commands

Command	Description
interface port-channel	Creates a port channel virtual interface and enters interface configuration mode.
port-channel load-defer	Configures the global port load share deferral time interval for port channels.
show etherchannel	Displays the EtherChannel information for a channel.

port-channel standalone-disable

To disable the EtherChannel standalone option in a port channel, use the **port-channel standalone-disable** command in interface configuration mode. To enable this option, use the **no** form of this command.

port-channel standalone-disable
no port-channel standalone-disable

Syntax Description

This command has no arguments or keywords.

Command Default

The EtherChannel standalone option is enabled.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.2(33)SXI3	This command was introduced.
15.1(1)SG	This command was integrated into Cisco IOS Release 15.1(1)SG.
Cisco IOS XE Release 3.3SG	This command was integrated into Cisco IOS XE Release 3.3SG.

Usage Guidelines

The **port-channel standalone-disable** command is supported on the Catalyst 6000 series switches. This command can be used only when the port-channel protocol type is Link Aggregation Control Protocol (LACP). This command enables you to change the current behavior when a physical port cannot bundle an LACP EtherChannel.

Examples

The following example shows how to disable the EtherChannel standalone option in a port channel:

```
Device(config-if)# port-channel standalone-disable
```

Related Commands

Command	Description
show etherchannel	Displays the EtherChannel information for a channel.

pos ais-shut

To send the line alarm indication signal (LAIS) when the Packet-over-SONET (POS) interface is placed in any administrative shutdown state, use the pos ais-shut command in interface configuration mode.

pos ais-shut

Syntax Description

This command has no arguments or keywords.

Command Default

No LAIS is sent.

Command Modes

Interface configuration

Command History

Release	Modification
11.1CC	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

In Automatic Protection Switching (APS) environments, LAIS can be used to force a protection switch. This command forces an APS switch when the interface is placed in the administrative shutdown state.

For more information on APS, refer to the “Configuring Serial Interfaces” chapter in the Cisco IOS Interface and Hardware Component Configuration Guide.

This command does not have a **no** form.

Examples

The following example forces the alarm indication on POS OC-3 interface 0 in slot 3:

```
Router(config)# interface pos 3/0
Router(config-if)# shutdown
Router(config-if)# pos ais-shut
```

pos delay triggers

To enable a POS alarm trigger delay, or to enable path level alarms as triggers to bring the POS line card protocol to down, use the pos delay triggers command in POS interface configuration mode. To disable POS alarm trigger delays, use the **no** form of this command.

pos delay triggers [**line** *ms* | **path** *ms*]
no pos delay triggers [**line** *ms* | **path** *ms*]

Syntax Description

line	Specifies the delay for SONET line level triggers. The following alarms are considered line level triggers: section loss of signal, section loss of frame, line alarm indication signal. SONET line level triggers bring the line protocol down by default
path	Specifies that SONET path level alarms should trigger the line protocol to go down.
ms	Specifies the time, in milliseconds, that POS trigger should wait before setting the line protocol to down. If no *ms* value is entered, the default value of 100 ms is used.

Command Default

POS line level alarm triggers are enabled by default. If a POS line level alarm trigger occurs and no configuration changes have been made using the**posdelaytriggersline***ms*command, the line protocol is set to down immediately with no delay.

POS path level alarm triggers are disabled by default. A path level alarm will not set the line protocol to down unless the **posdelaytriggerspath** command has been entered.

If no *ms* value is entered but **posdelaytriggersline** command is configured, the default *ms* value for line level triggers is 100 ms.

If no *ms* value is entered and **posdelaytriggerspath** is enabled, the default *ms* value is set at 100 ms for path level triggers.

Command Modes

POS interface configuration

Command History

Release	Modification
12.1(12c)EX1	This command was introduced for Cisco 7304 routers.
12.2(18)S	This command was introduced on Cisco 7304 routers running Cisco IOS Release 12.2S.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command was integrated into Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
12.4	This command was integrated into Cisco IOS Release 12.4 Mainline. This command supports Cisco 7200 Series, Cisco 7304 Series, and Cisco 7600 Series routers.
12.4(24)T	This command was integrated into a release earlier than Cisco IOS Release 12.4(24)T. This command supports Cisco 7200 Series, Cisco 7304 Series, and Cisco 7600 Series routers.

Usage Guidelines

A trigger is an alarm that, when asserted, causes the line protocol to go down.

When one or more triggers are asserted, the line protocol of the interface goes down. The POS Alarm Trigger Delay feature provides the option to delay triggering of the line protocol of the interface from going down when an alarm triggers the line protocol to go down. For instance, if you configure the POS alarm delay for 150 ms, the line protocol will not go down for 150 ms after receiving the trigger. If the trigger alarm stays up for more than 150 ms, the link is brought down as it is now. If the trigger alarm clears before 150 ms, the line protocol is not brought down.

By default, the following line and section alarms are triggers for the line protocol to go down:

- Section loss of signal
- Section loss of frame
- Line alarm indication signal

For line and section alarm triggers, the line protocol of the POS card is brought down immediately if a trigger is received and no POS alarm trigger delay is specified. The delay can be set anywhere from 50 to 10000 ms. If POS alarm triggering is configured but no *ms* value is entered, the POS alarm trigger delay is 100 ms.

The following path alarms are not triggers by default. These path alarms, however, can be configured as triggers:

- Path alarm indication signal
- Path remote defect indication

The POS Alarm Trigger Delay feature can be used to configure these alarms as triggers, as well as to configure the exact POS alarm trigger delay for these triggers. The default delay values for these triggers, if no value is specified, is also 100 ms.

Examples

In the following configuration example, the POS line card will wait 50 ms after receiving a line level trigger before setting the line protocol to down. If the alarm that began the line level trigger clears during that 50 ms, the line protocol will remain up. If the alarm that began the line trigger remains after that 50 ms, the line protocol will go down.

```
Router# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)# interface pos 1/0
Router(config-if)# pos delay triggers line 50
```

In the following configuration example, the POS line card will wait 110 ms after receiving a path trigger before setting the line protocol to down. If the alarm that began the path trigger clears during that 110 ms, the line protocol will remain up. If the alarm that began the path trigger remains after 110 ms, the line protocol will go down.

```
Router# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)# interface pos 1/0
Router(config-if)# pos delay triggers path 110
```

In the following example, the **showcontrollerspos***slot*/*interface-number***detail** command is used to verify the POS alarm trigger delay. In this particular example, the delay is 100 ms (italicized for emphasis below) for both line level triggers and path level triggers.

```
Router# show controllers pos 4/0 detail
```

POS4/0

SECTION

LOF = 0 LOS = 0 BIP(B1) = 22

LINE

AIS = 0 RDI = 0 FEBE = 21 BIP(B2) = 38

PATH

AIS = 0 RDI = 1 FEBE = 25 BIP(B3) = 31

PLM = 0 UNEQ = 0 TIM = 0 TIU = 0

LOP = 0 NEWPTR = 4 PSE = 2 NSE = 3

Active Defects:None

Active Alarms: None

Alarm reporting enabled for:SF SLOS SLOF B1-TCA B2-TCA PLOP B3-TCA

Line triggers delayed 100 ms

```
Path triggers delayed 100 ms
...
```

Related Commands

Command	Description
show controllers pos *slot* / *interface-number* **detail**	Shows the content of POS controllers, including the amount of delay for line triggers.

pos flag

To set the SONET overhead bytes in the frame header to meet a specific standards requirement or to ensure interoperability with the equipment of another vendor, use the **posflag**command in interface configuration mode. To remove the setting of the SONET overhead bytes, use the **no** form of this command.

pos flag commandpos flag {**c2** | **j0** | **s1s0**} *value*
no pos flag {**c2** | **j0** | **s1s0**} *value*

Syntax Description

c2 *value*	Path signal identifier used to identify the payload content type. The default value is 0xCF.
j0 *value*	Section trace byte (formerly the C1 byte). For interoperability with Synchronous Digital Hierarchy (SDH) equipment in Japan, use the value 0x1. The byte value can be 0 to 255.
sls0 *value*	S1 and S0 bits (bits 5 and 6 of the H1 #1 payload pointer byte). Use the following values to tell the SONET transmission equipment the SS bit: • For OC-3c, use 0 (this is the default). • For AU-4 container in SDH, use 2. The S1 and S0 bits can be 0 to 3. Values 1 and 3 are undefined. The default value is 0.

Command Default

The default **c2** value is 0xCF. The default **sls0** value is 0.

Command Modes

Interface configuration

Command History

Release	Modification
11.2 GS	This command was introduced to support the Cisco 12000 series Internet routers.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Use the following values to tell the SONET transmission equipment the payload type:

- For PPP, or High-Level Data Link Control (HDLC) when required, use 0xCF (this is the default).
- For ATM, use 0x13.
- For other equipment, use any nonzero value.
- The byte value can be 0 to 255.

Examples

The following example sets the path signal identifier used to identify the payload content type to ATM on the **pos** interface in slot 9:

```
Router(config)# interface pos 9/0
```

```
Router(config-if)# pos flag c2 0x13
Router(config-if)# end
```

pos flag s1-byte rx-communicate

To direct the router to switch to internal clocking when it receives an S1 SONET overhead byte with a value of 0xF, use the pos flag s1-byte rx-communicate command in interface configuration mode. To disable this capability, use the **no** form of this command.

pos flag s1-byte rx-communicate
no pos flag s1-byte rx-communicate

Command Default

Disabled

Command Modes

Interface configuration

Command History

Release	Modification
12.2(28)SB	This command was introduced on the Cisco 10000 series router.

Usage Guidelines

The pos flag s1-byte rx-communicate command directs the router to switch the clock source to internal when it receives an S1 SONET overhead byte with a value of 0xF. When the S1 SONET overhead byte changes from 0xF to any other value, the clock source reverts back to the clock source specified in the user configuration.

The S1 SONET overhead byte is ignored by the receiving router unless the pos flag s1-byte rx-communicate command is issued.

Examples

The following example directs the router to switch to internal clocking when it receives an S1 SONET overhead byte with a value of 0xF:

```
pos flag s1-byte rx-communicate
```

Related Commands

Command	Description
pos flag	Assigns values for specific elements of the frame header. This command is typically used to meet a standards requirement or to ensure interoperability with another vendor's equipment.
pos flag s1-byte tx	Controls the transmission of the S1 SONET overhead byte.

pos flag s1-byte tx

To control the transmission of the S1 SONET overhead byte, use the pos flag s1-byte tx command in interface configuration mode.

pos flag s1-byte tx *value*

Syntax Description

value	Set the S1 SONET overhead byte to a value in the range of 0x0 to 0xF.

Command Default

The default is 0x0.

Command Modes

Interface configuration

Command History

Release	Modification
12.2(28)SB	This command was introduced on the Cisco 10000 series router.

Usage Guidelines

In most situations, the default value for the S1 SONET overhead byte does not need to be changed. Refer to the SONET standards for information about the possible values for the S1 SONET overhead byte and the definition of each value.

Examples

The following example sets the S1 SONET overhead byte to 0xF:

```
pos flag s1-byte tx 0xF
```

Related Commands

Command	Description
pos flag	Assigns values for specific elements of the frame header. This command is typically used to meet a standards requirement or to ensure interoperability with another vendor's equipment.
pos flag s1-byte rx-communicate	Directs the router to switch to internal clocking when it receives an S1 SONET overhead byte with a value of 0xF.

pos framing

To specify the framing used on the POS (Packet-over-SONET) interface, use the **posframing** command in interface configuration mode. To return to the default SONET STS-3c framing mode, use the **no** form of this command.

pos framing commandpos framing {**sdh** | **sonet**}
no pos framing

Syntax Description

sdh	Selects SDH STM-1 framing. This framing mode is typically used in Europe.
sonet	Selects SONET STS-3c framing. This is the default.

Command Default

SONET STS-3c framing

Command Modes

Interface configuration

Command History

Release	Modification
11.2	This command was introduced.
11.3	This command was modified to change the **posiframing-sdh** command to **posframing-sdh**.
11.2GS	The command syntax was changed from **posframing-sdh** to **posframing**. The **sonet** keyword was added.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Examples

The following example configures the interface for SDH STM-1 framing:

```
Router(config)# interface pos 3/0
Router(config-if)# pos framing sdh
Router(config-if)# no shutdown
```

Related Commands

Command	Description
clock source (interface)	Controls the clock used by a G.703-E1 interface.
interface	Configures an interface type, and enters interface configuration mode.

pos report

To permit selected SONET alarms to be logged to the console for a POS (Packet-over-SONET) interface, use the **posreport**command in interface configuration mode. To disable logging of select SONET alarms, use the **no** form of this command.

pos report commandpos report {**b1-tca** | **b2-tca** | **b3-tca** | **lais** | **lrdi** | **pais** | **plop** | **prdi** | **rdool** | **sd-ber** | **sf-ber** | **slof** | **slos**}
no pos report {**b1-tca** | **b2-tca** | **b3-tca** | **lais** | **lrdi** | **pais** | **plop** | **prdi** | **rdool** | **sd-ber** | **sf-ber** | **slof** | **slos**}

Syntax Description

b1-tca	Reports B1 bit-error rate (BER) threshold crossing alarm (TCA) errors.
b2-tca	Reports B2 BER crossing TCA errors.
b3-tca	Reports B3 BER crossing TCA errors.
lais	Reports line alarm indication signal errors.
lrdi	Reports line remote defect indication errors.
pais	Reports path alarm indication signal errors.
plop	Reports path loss of pointer errors.
prdi	Reports path remote defect indication errors.
rdool	Reports receive data out of lock errors.
sd-ber	Reports signal degradation BER errors.
sf-ber	Reports signal failure BER errors.
slof	Reports section loss of frame errors.
slos	Reports section los of signal errors.

Command Default

The following alarms are reported by default:

- **b1-tca**
- **b2-tca**
- **b3-tca**
- **plop**
- **sf-ber**
- **slof**
- **slos**

Command Modes

Interface configuration

Command History

Release	Modification
11.1CC	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Reporting an alarm means that the alarm can be logged to the console. Just because an alarm is permitted to be logged does not guarantee that it is logged. SONET alarm hierarchy rules dictate that only the most severe alarm of an alarm group is reported. Whether an alarm is reported or not, you can view the current state of a defect by checking the "Active Defects" line from the **showcontrollerspos**command output. A defect is a problem indication that is a candidate for an alarm.

For B1, the bit interleaved parity error report is calculated by comparing the BIP-8 code with the BIP-8 code extracted from the B1 byte of the following frame. Differences indicate that section level bit errors have occurred.

For B2, the bit interleaved parity error report is calculated by comparing the BIP-8/24 code with the BIP-8 code extracted from the B2 byte of the following frame. Differences indicate that line level bit errors have occurred.

For B3, the bit interleaved parity error report is calculated by comparing the BIP-8 code with the BIP-8 code extracted from the B3 byte of the following frame. Differences indicate that path level bit errors have occurred.

PAIS is sent by line terminating equipment (LTE) to alert the downstream path terminating equipment (PTE) that it has detected a defect on its incoming line signal.

PLOP is reported as a result of an invalid pointer (H1, H2) or an excess number of new data flag (NDF) enabled indications.

SLOF is detected when a severely error framing (SEF) defect on the incoming SONET signal persists for 3 milliseconds.

SLOS is detected when an all-zeros pattern on the incoming SONET signal lasts 19 plus or minus 3 microseconds or longer. This defect might also be reported if the received signal level drops below the specified threshold.

To determine the alarms that are reported on the interface, use the **showcontrollerspos**command.

Examples

The following example enables reporting of SD-BER and LAIS alarms on the interface:

```
Router(config)# interface pos 3/0/0
Router(config-if)# pos report sd-ber
Router(config-if)# pos report lais
Router(config-if)# end
```

Related Commands

Command	Description
interface	Configures an interface type, and enters interface configuration mode.
show controllers pos	Displays information about the POS controllers.

pos scramble-atm

To enable SONET payload scrambling on a POS (Packet-over-SONET) interface, use the **posscramble-atm**command in interface configuration mode. To disable scrambling, use the **no** form of this command.

pos scramble-atm commandpos scramble-atm
no pos scramble-atm

Syntax Description

This command has no arguments or keywords.

Command Default

Scrambling is disabled.

Command Modes

Interface configuration

Command History

Release	Modification
11.1CA	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

SONET payload scrambling applies a self-synchronous scrambler (x43+1) to the Synchronous Payload Envelope (SPE) of the interface to ensure sufficient bit transition density. Both ends of the connection must use the same scrambling algorithm. When enabling POS scrambling on a VIP2 POSIP on the Cisco 7500 series router that has a hardware revision of 1.5 or higher, you can specify CRC 16 only (that is, CRC 32 is currently not supported).

To determine the hardware revision of the POSIP, use the **showdiag** command.

To determine whether scrambling is enabled on the interface, use the **showinterfacepos** command or the **showrunning-config** command.



Note SONET payload scrambling is enabled with the **posscramble-atm** command. SONET payload scrambling applies a self-synchronous scrambler (x43+1) to the Synchronous Payload Envelope (SPE) of the interface to ensure sufficient bit transition density. Both sides of the connection must be configured using the **posscramble-atm** command. Currently, when connecting to a Cisco 7500 series router and using the **posscramble-atm** command, you must specify the **crc16** command rather than the **crc32** command.

Examples

The following example enables scrambling on the interface:

```
Router(config)# interface pos 3/0
Router(config-if)# pos scramble-atm
Router(config-if)# no shutdown
Router(config-if)# end
```

Related Commands

Command	Description
crc	Sets the length of the CRC on an FSIP or HIP of the Cisco 7500 series routers or on a 4-port serial adapter of the Cisco 7200 series routers.
interface	Configures an interface type, and enters interface configuration mode.
show diag	Displays hardware information for the router.
show interfaces pos	Displays information about the Packet OC-3 interface in Cisco 7500 series routers.

pos threshold

To set the bit-error rate (BER) threshold values of the specified alarms for a POS (Packet-Over-SONET) interface, use the **posthreshold**command in interface configuration mode. To return to the default setting, use the **no** form of this command.

pos threshold {**b1-tca** | **b2-tca** | **b3-tca** | **sd-ber** | **sf-ber**} *rate*
no pos threshold {**b1-tca** | **b2-tca** | **b3-tca** | **sd-ber** | **sf-ber**} *rate*

Syntax Description

b1-tca	B1 BER threshold crossing alarm. The default rate is 6.
b2-tca	B2 BER threshold crossing alarm. The default rate is 6.
b3-tca	B3 BER threshold crossing alarm. The default rate is 6.
sd-ber	Signal degrade BER threshold. The default rate is 6.
sf-ber	Signal failure BER threshold. The default rate is 3 (10e-3).
rate	Bit-error rate from 3 to 9 (10-n).

Command Default

The default rate is 6 for **b1-tca**, **b2-tca**, **b3-tca**, and **sd-ber**. The default rateis 3 (10e-3) for **sf-ber**.

Command Modes

Interface configuration

Command History

Release	Modification
11.1CC	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

For B1, the bit interleaved parity error report is calculated by comparing the BIP-8 code with the BIP-8 code extracted from the B1 byte of the following frame. Differences indicate that section level bit errors have occurred.

For B2, the bit interleaved parity error report is calculated by comparing the BIP-8/24 code with the BIP-8 code extracted from the B2 byte of the following frame. Differences indicate that line level bit errors have occurred.

For B3, the bit interleaved parity error report is calculated by comparing the BIP-8 code with the BIP-8 code extracted from the B3 byte of the following frame. Differences indicate that path level bit errors have occurred.

SF-BER and SD-BER are sourced from B2 BIP-8 error counts (as is B2-TCA). However, SF-BER and SD-BER feed into the automatic protection switching (APS) machine and can lead to a protection switch (if APS is configured).

B1-TCA, B2-TCA, and B3-TCA do nothing more than print a log message to the console (if reports for them are enabled).

To determine the BER thresholds configured on the interface, use the **showcontrollerspos**command.

Examples

The following example configures thresholds on the interface:

```
Router(config)# interface pos 3/0/0
Router(config-if)# pos threshold sd-ber 8
Router(config-if)# pos threshold sf-ber 4
Router(config-if)# pos threshold b1-tca 4
Router(config-if)# end
```

Related Commands

Command	Description
interface	Configures an interface type, and enters interface configuration mode.
pos report	Permits selected SONET alarms to be logged to the console for a POS interface.
show controllers pos	Displays information about the POS controllers.

power inline

To determine how inline power is applied to the device on the specified switch port, use the **powerinline** command in interface configuration mode. To return the setting to its default, use the **no** form of this command.

power inline {**auto** [**max** *max-milliwatts*] | **never** | **police** | **static** [**max** *max-milliwatts*]}
no power inline [**police**]

Cisco Integrated Services Routers Generation 2 (ISR G2) with Cisco Gigabit EtherSwitch enhanced high-speed WAN interface cards (EHWICs)
power inline {**auto** | **never** | **port max** *max-milliwatts*}
no power inline {**auto** | **never** | **port max** *max-milliwatts*}

Cisco 4451-X Integrated Services Router
power inline
auto | [**max** *max-milliwatts*] | **never** | **redundant**
no power inline
auto | [**max** *max-milliwatts*] | **never** | **redundant**

Syntax Description

auto	Turns on the device discovery protocol and applies power to the device, if found.
max *max-milliwatts*	(Optional) Specifies the maximum amount of power, in milliwatts, that a device connected to a port can consume. Range: 4000 to 16800. Default: 15400.
never	Turns off the device discovery protocol and stops supplying power to the device.
police	Turns on inline power policing; optional if entering the **no** form of the command. Default is disabled.
static	Allocates power from the system power pool to a port.
port max *max-milliwatts*	Specifies the maximum power allocated to the port. The maximum power can be set between 4,000 to 20,000 milliwatts.
redundant	Puts the inline power supply in redundant mode (default mode). (For boost mode, use the no form of the command; for example, **no power inline redundant**.)

Command Default

Power is applied when a telephone is detected on the port (**auto**).*max-milliwatts* is 15400 milliwatts. Inline power policing is disabled.

Power is applied when a telephone is detected on the port (auto). The maximum power limit is 20000 milliwatts. Inline power policing is disabled.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.0(5)XU	This command was introduced.
12.2(2)XT	This command was integrated to support switchport creation on Cisco 2600 series, Cisco 3600 series, and Cisco 3700 series routers.
12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T to support switchport creation .
12.2(14)SX	Support for this command was introduced on the Supervisor Engine 720.
12.2(17b)SXA	This command was changed to include the **static** and **max***max-milliwatts* keywords and arguments.
12.2(17d)SXB	Support for this command on the Supervisor Engine 2 was extended to Cisco IOS Release 12.2(17d)SXB.
12.2(33)SXH	This command was changed to include the **police** keyword .
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH2	This command was changed to increase the *max-watts* maximum to 16800 milliwatts for the WS-F6K-48-AF and the WS-F6K-GE48-AF modules. The default setting remains 15400 milliwatts. See the “Usage Guidelines” section for additional information.
15.1(2)T	This command was modified. The **portmax**keyword and *max-milliwatts* argument were added.
Cisco IOS XE Release 3.9S	This command was integrated into Cisco IOS XE Release 3.9S.

Usage Guidelines

The **police**keyword appears if you have a WS-F6K-48-AF or other inline power daughter card that supports power monitoring and inline power policing.

Inline power is supported only on switch ports that are connected to an IP phone. Before you enable inline power on a switch port, you must enter the **switchport** command.

The following information applies to WS-F6K-48-AF and WS-F6K-GE48-AF inline power cards:

- In Cisco IOS Release 12.2(33)SXH2 and later releases, the configurable range of maximum power using the max keyword is 4000 to 16800 milliwatts. For earlier releases, the configurable range for maximum power is 4000 to 15400 milliwatts. For all releases, if no maximum power level is configured, the default maximum power is 15400 milliwatts.



Note To support a large number of inline-powered ports using power levels above 15400 milliwatts on an inline power card, we recommend using the static keyword so that the power budget is deterministic.

- In Cisco IOS Release 12.2(33)SXH2 and later releases, when you enter the auto keyword and CDP is enabled on the port, an inline-powered device that supports CDP can negotiate a power level up to 16800 milliwatts unless a lower maximum power level is configured. For earlier releases, the inline-powered

device can negotiate a power level up to 15400 milliwatts or the configured maximum power level, if it is configured lower than 15400 milliwatts.

Cisco ISR G2 with Cisco Gigabit EHWICs

- The **portmax**keyword and *max-milliwatts* argument are available only on the Firebee cards with Power-over-Ethernet (PoE).

Examples

The following example shows how to set the inline power to the off mode on a switch port:

```
Router(config)# interface fastethernet5/1
Router(config-if)# switchport
Router(config-if)# power inline never
```

The following example shows how to allocate power from the system power pool to a switch port:

```
Router(config)# interface fastethernet5/1
Router(config-if)# switchport
Router(config-if)# power inline static max 15000
```

The following example shows how to turn on inline power policing to a switch port:

```
Router(config)# interface gigabitethernet6/3
Router(config-if)# switchport
Router(config-if)# power inline police
```

Cisco ISR G2 with Cisco Gigabit EtherSwitch EHWICs

The following example shows how to turn on inline power to a switch port:

```
Router(config)# interface gigabitethernet
0/1/3
Router(config-if)#
power inline
auto{!-condition!}
```

The following example shows how to set maximum inline power to a switch port:

```
Router(config)# interface
 gigabitethernet
0/1/3
```

The following example shows how to disable inline power to the switch port:

```
Router(config)# interface
 gigabitethernet

0/1/3
Router(config-if)# power inline
 never{!-condition!}
```

Cisco 4451-X Integrated Service Router

The following example shows auto option for power inline command configured on the front panel Gigabit Ethernet port.

```
Router(config)# interface gigabitEthernet 0/0/0
Router(config-if)# power inline auto
```

In this example, an attempt is made to configure the inline power to be in boost mode by using the **no** form of the **power inline redundant** command. The inline power mode is not changed to boost mode because that requires a total power available in redundant mode of 1000W.

```
Router# show power
Main PSU :
Configured Mode : Boost
Current runtime state same : Yes
Total power available : 2000 Watts
POE Module :
Configured Mode : Boost
Current runtime state same : Yes
Total power available : 1000 Watts
Router# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)# no power inline redundant
*Jan 31 03:42:40.947: %PLATFORM_POWER-6-MODEMISMATCH: Inline power not in Boost mode
Router(config)# exit
*Jan 31 03:36:13.111: %SYS-5-CONFIG_I: Configured from console by console
Router# show power
Main PSU :
Configured Mode : Boost
Current runtime state same : Yes
Total power available : 1450 Watts
POE Module :
Configured Mode : Boost
Current runtime state same : No
Total power available : 500 Watts
```

In this example, power for the main power supply is configured to be in boost mode by using the **no** form of the **power main redundant** command. This sets the power for the main power supply in boost mode to be 1450 W and the inline power in redundant mode as 500W.

```
Router# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)# no power main redundant
Router(config)#
*Jan 31 03:35:22.284: %PLATFORM_POWER-6-MODEMATCH: Inline power is in Redundant mode
Router(config)#
Router(config)# exit
Router#
*Jan 31 03:36:13.111: %SYS-5-CONFIG_I: Configured from console by console
Router# show power
Main PSU :
Configured Mode : Boost
Current runtime state same : Yes
Total power available : 1450 Watts
POE Module :
Configured Mode : Redundant
Current runtime state same : Yes
Total power available : 500 Watts
Router#
```

Related Commands

Command	Description
show power inline	Displays the power status for the specified port or for all ports.
switchport priority extend	Determines how the telephone connected to the specified port handles priority traffic received on its incoming port.
switchport voice vlan	Configures the voice VLAN on the port.

power enable

To turn on power for the modules, use the **power enable**command in global configuration mode. To power down a module, use the **no** form of this command.

power enable module *slot*
no power enable module *slot*

Syntax Description

module *slot*	Specifies a module slot number; see the "Usage Guidelines" section for valid values.

Command Default

Enabled

Command Modes

Global configuration

Command History

Release	Modification
12.2(14)SX	Support for this command was introduced on the Supervisor Engine 720.
12.2(17d)SXB	Support for this command on the Supervisor Engine 2 was extended to Release 12.2(17d)SXB.
12.2(18)SXD	This command was changed to allow you to disable power to empty slots.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

When you enter the **no power enable module** *slot* command to power down a module, the module's configuration is not saved.

When you enter the **no power enable module** *slot* command to power down an empty slot, the configuration is saved.

The *slot* argument designates the module number. Valid values for *slot*depend on the chassis that is used. For example, if you have a 13-slot chassis, valid values for the module number are from 1 to 13.

Examples

This example shows how to turn on the power for a module that was previously powered down:

```
Router(config)#
power enable module 5
Router(config)#
```

This example shows how to power down a module:

```
Router(config)#
no power enable module 5
Router(config)#
```

Related Commands

Command	Description
show power	Displays information about the power status.

power inline

To determine how inline power is applied to the device on the specified switch port, use the **powerinline** command in interface configuration mode. To return the setting to its default, use the **no** form of this command.

power inline {**auto** [**max** *max-milliwatts*] | **never** | **police** | **static** [**max** *max-milliwatts*]}
no power inline [**police**]

Cisco Integrated Services Routers Generation 2 (ISR G2) with Cisco Gigabit EtherSwitch enhanced high-speed WAN interface cards (EHWICs)
power inline {**auto** | **never** | **port max** *max-milliwatts*}
no power inline {**auto** | **never** | **port max** *max-milliwatts*}

Cisco 4451-X Integrated Services Router
power inline
auto | [**max** *max-milliwatts*] | **never** | **redundant**
no power inline
auto | [**max** *max-milliwatts*] | **never** | **redundant**

Syntax Description

auto	Turns on the device discovery protocol and applies power to the device, if found.
max *max-milliwatts*	(Optional) Specifies the maximum amount of power, in milliwatts, that a device connected to a port can consume. Range: 4000 to 16800. Default: 15400.
never	Turns off the device discovery protocol and stops supplying power to the device.
police	Turns on inline power policing; optional if entering the **no** form of the command. Default is disabled.
static	Allocates power from the system power pool to a port.
port max *max-milliwatts*	Specifies the maximum power allocated to the port. The maximum power can be set between 4,000 to 20,000 milliwatts.
redundant	Puts the inline power supply in redundant mode (default mode). (For boost mode, use the no form of the command; for example, **no power inline redundant**.)

Command Default

Power is applied when a telephone is detected on the port (**auto**).*max-milliwatts* is 15400 milliwatts. Inline power policing is disabled.

Power is applied when a telephone is detected on the port (auto). The maximum power limit is 20000 milliwatts. Inline power policing is disabled.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.0(5)XU	This command was introduced.
12.2(2)XT	This command was integrated to support switchport creation on Cisco 2600 series, Cisco 3600 series, and Cisco 3700 series routers.
12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T to support switchport creation .
12.2(14)SX	Support for this command was introduced on the Supervisor Engine 720.
12.2(17b)SXA	This command was changed to include the **static** and **max***max-milliwatts* keywords and arguments.
12.2(17d)SXB	Support for this command on the Supervisor Engine 2 was extended to Cisco IOS Release 12.2(17d)SXB.
12.2(33)SXH	This command was changed to include the **police** keyword .
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH2	This command was changed to increase the *max-watts* maximum to 16800 milliwatts for the WS-F6K-48-AF and the WS-F6K-GE48-AF modules. The default setting remains 15400 milliwatts. See the “Usage Guidelines” section for additional information.
15.1(2)T	This command was modified. The **portmax**keyword and *max-milliwatts* argument were added.
Cisco IOS XE Release 3.9S	This command was integrated into Cisco IOS XE Release 3.9S.

Usage Guidelines

The **police**keyword appears if you have a WS-F6K-48-AF or other inline power daughter card that supports power monitoring and inline power policing.

Inline power is supported only on switch ports that are connected to an IP phone. Before you enable inline power on a switch port, you must enter the **switchport** command.

The following information applies to WS-F6K-48-AF and WS-F6K-GE48-AF inline power cards:

- In Cisco IOS Release 12.2(33)SXH2 and later releases, the configurable range of maximum power using the max keyword is 4000 to 16800 milliwatts. For earlier releases, the configurable range for maximum power is 4000 to 15400 milliwatts. For all releases, if no maximum power level is configured, the default maximum power is 15400 milliwatts.



Note To support a large number of inline-powered ports using power levels above 15400 milliwatts on an inline power card, we recommend using the static keyword so that the power budget is deterministic.

- In Cisco IOS Release 12.2(33)SXH2 and later releases, when you enter the auto keyword and CDP is enabled on the port, an inline-powered device that supports CDP can negotiate a power level up to 16800 milliwatts unless a lower maximum power level is configured. For earlier releases, the inline-powered

device can negotiate a power level up to 15400 milliwatts or the configured maximum power level, if it is configured lower than 15400 milliwatts.

Cisco ISR G2 with Cisco Gigabit EHWICs

- The **portmax**keyword and *max-milliwatts* argument are available only on the Firebee cards with Power-over-Ethernet (PoE).

Examples

The following example shows how to set the inline power to the off mode on a switch port:

```
Router(config)# interface fastethernet5/1
Router(config-if)# switchport
Router(config-if)# power inline never
```

The following example shows how to allocate power from the system power pool to a switch port:

```
Router(config)# interface fastethernet5/1
Router(config-if)# switchport
Router(config-if)# power inline static max 15000
```

The following example shows how to turn on inline power policing to a switch port:

```
Router(config)# interface gigabitethernet6/3
Router(config-if)# switchport
Router(config-if)# power inline police
```

Cisco ISR G2 with Cisco Gigabit EtherSwitch EHWICs

The following example shows how to turn on inline power to a switch port:

```
Router(config)# interface gigabitethernet
0/1/3
Router(config-if)#
power inline
auto{!-condition!}
```

The following example shows how to set maximum inline power to a switch port:

```
Router(config)# interface
 gigabitethernet
0/1/3
```

The following example shows how to disable inline power to the switch port:

```
Router(config)# interface
 gigabitethernet

0/1/3
Router(config-if)# power inline
 never{!-condition!}
```

Cisco 4451-X Integrated Service Router

The following example shows auto option for power inline command configured on the front panel Gigabit Ethernet port.

```
Router(config)# interface gigabitEthernet 0/0/0
Router(config-if)# power inline auto
```

In this example, an attempt is made to configure the inline power to be in boost mode by using the **no** form of the **power inline redundant** command. The inline power mode is not changed to boost mode because that requires a total power available in redundant mode of 1000W.

```
Router# show power
Main PSU :
Configured Mode : Boost
Current runtime state same : Yes
Total power available : 2000 Watts
POE Module :
Configured Mode : Boost
Current runtime state same : Yes
Total power available : 1000 Watts
Router# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)# no power inline redundant
*Jan 31 03:42:40.947: %PLATFORM_POWER-6-MODEMISMATCH: Inline power not in Boost mode
Router(config)# exit
*Jan 31 03:36:13.111: %SYS-5-CONFIG_I: Configured from console by console
Router# show power
Main PSU :
Configured Mode : Boost
Current runtime state same : Yes
Total power available : 1450 Watts
POE Module :
Configured Mode : Boost
Current runtime state same : No
Total power available : 500 Watts
```

In this example, power for the main power supply is configured to be in boost mode by using the **no** form of the **power main redundant** command. This sets the power for the main power supply in boost mode to be 1450 W and the inline power in redundant mode as 500W.

```
Router# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)# no power main redundant
Router(config)#
*Jan 31 03:35:22.284: %PLATFORM_POWER-6-MODEMATCH: Inline power is in Redundant mode
Router(config)#
Router(config)# exit
Router#
*Jan 31 03:36:13.111: %SYS-5-CONFIG_I: Configured from console by console
Router# show power
Main PSU :
Configured Mode : Boost
Current runtime state same : Yes
Total power available : 1450 Watts
POE Module :
Configured Mode : Redundant
Current runtime state same : Yes
Total power available : 500 Watts
Router#
```

Related Commands

Command	Description
show power inline	Displays the power status for the specified port or for all ports.
switchport priority extend	Determines how the telephone connected to the specified port handles priority traffic received on its incoming port.
switchport voice vlan	Configures the voice VLAN on the port.

power redundancy-mode

To set the power-supply redundancy mode, use the **power redundancy-mode** command in global configuration mode.

power redundancy-mode {**combined** | **redundant**}

Syntax Description

combined	Specifies no redundancy (combine power-supply outputs).
redundant	Specifies redundancy (either power supply can operate the system).

Command Default

redundant

Command Modes

Global configuration

Command History

Release	Modification
12.2(14)SX	Support for this command was introduced on the Supervisor Engine 720.
12.2(17d)SXB	Support for this command on the Supervisor Engine 2 was extended to Release 12.2(17d)SXB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Examples

This example shows how to set the power supplies to the no-redundancy mode:

```
Router(config)#
power redundancy-mode combined
Router(config)#
```

This example shows how to set the power supplies to the redundancy mode:

```
Router(config)#
power redundancy-mode redundant
Router(config)#
```

Related Commands

Command	Description
show power	Displays information about the power status.

ppp link

To generate the Point-to-Point Protocol (PPP) Link Control Protocol (LCP) down and keepalive-failure link traps or enable calls to the interface-reset vector, use the **ppplink**command in interface configuration mode. To disable the PPP LCP down and keepalive-failure link traps or calls to the interface-reset vector, use the **no** form of this command.

ppp link {**reset** | **trap**}
no ppp link {**reset** | **trap**}

Syntax Description

reset	Specifies calls to the interface reset vector.
trap	Specifies the PPP LCP down and keepalive-failure link traps.

Command Default

The defaults are as follows:

- The calls are sent to the interface-reset vector.
- The traps are sent when the LCP goes down.

Command Modes

Interface configuration

Command History

Release	Modification
12.2(17d)SXB	Support for this command on the Supervisor Engine 2 was extended to Release 12.2(17d)SXB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

This command is not supported on Cisco 7600 series routers that are configured with a Supervisor Engine 720.

The **noppplinktrap** command disables the sending of the link traps when the LCP goes down.

In the event that the PPP calls the interface-reset vector while the LCP is configured or closed, Up/Down status messages will display on the console. If a leased-line configuration is up but the peer is not responding, PPP may call the interface-reset vector once per minute. This situation may result in the Up/Down status messages on the console. Use the **noppplinkreset**command to disable calls to the interface-reset vector. PPP will continue to attempt to negotiate with the peer, but the interface will not be reset between each attempt.

Examples

This example shows how to enable calls to the interface-reset vector:

```
Router(config-if)#
ppp link reset
Router(config-if)#
```

This example shows how to disable calls to the interface-reset vector:

```
Router(config-if)#
no ppp link reset
Router(config-if)#
```

This example shows how to generate the PPP LCP down/keepalive-failure link traps:

```
Router(config-if)#
ppp link trap
Router(config-if)#
```

This example shows how to disable the sending of the link traps when the LCP goes down:

```
Router(config-if)#
no ppp link trap
Router(config-if)#
```

ppp loopback no-backoff

To enable continuous Link Control Protocol (LCP) negotiation of loopback links with PPP sessions, use the **ppp loopback no-backoff** command in interface configuration mode. To restrict negotiation of loopback links with PPP sessions to ten LCP Configure Request (CONFREQ) messages, use the **no** form of this command.

ppp loopback no-backoff

no ppp loopback no-backoff

Command Default Loopback links with PPP sessions disconnect after ten LCP CONFREQ messages are sent for negotiation.

Command Modes Interface configuration (config-if)

Command History

Release	Modification
Cisco IOS XE Release 3.10.1S	This command was introduced.

Usage Guidelines A circuit loopback indicates wiring issues in a device or faults with external switching equipment. The default functionality of the PPP protocol is to check for loopbacks and disconnect the session link when a loopback is detected. The PPP protocol includes a mechanism that detects a circuit loopback; that is, it detects a situation when a circuit feeds back upon itself, which results in the device reading its own output on that link. The first phase of loopback detection occurs during LCP negotiation when the circuit is being established. If you enable keepalives on a link, the second phase of loopback detection occurs after the connection is established.

Note Loopback detection depends upon successful negotiation of the LCP magic number during link establishment. LCP magic numbers are used in PPP to avoid frame loopbacks.

Use the **ppp loopback no-backoff** command when it becomes essential to prevent disconnection of session links whenever a loopback is detected. This ensures that the link does not go down and that there is a continuous attempt to establish connection. Link negotiations continue until a unique LCP magic number is received. The **no** form of this command restores the default behavior in which the loopback links with PPP sessions disconnect after only ten LCP CONFREQ messages are sent for negotiation.

Example

The following example shows how to enable the **ppp loopback no-backoff** command on a serial interface:

```
Device> enable
Device# configure terminal
Device(config)# interface Serial1/0/0:1
Device(config-if)# no ip address
Device(config-if)# encapsulation ppp
Device(config-if)# ppp loopback no-backoff
Device(config-if)# end
```

Related Commands

Command	Description
encapsulation ppp	Enables PPP on an interface.
no ip address	Removes an IP address or disables IP processing.
ppp loopback ignore	Disables PPP loopback detection.

ppp multilink mrru

To configure the maximum receive reconstructed unit (MRRU) value negotiated on a Multilink PPP (MLP) bundle, use the **pppmultilinkmrru**command in interface configuration mode. To remove the configured MRRU, use the **no** form of this command.

ppp multilink mrru [**local** | **remote**] **bytes**
no ppp multilink mrru [**local** | **remote**] **bytes**

Syntax Description

local	(Optional) Configures the local MRRU value.
remote	(Optional) Configures the minimum value that the software will accept from the peer when it advertises its MRRU.
bytes	MRRU value, in bytes. Valid value range is 128 to 16384.

Command Default

The default values for the local MRRU are the value of the multilink group interface maximum transmission unit (MTU) for multilink group members, and 1524 bytes for all other interfaces.

Command Modes

Interface configuration

Command History

Release	Modification
12.3(7)T	This command was introduced.
12.0(28)S	This command was integrated into Cisco IOS Release 12.0(28)S.
12.2(27)SB	This command was integrated into Cisco IOS Release 12.2(27)SB.
12.2(28)S	This command was integrated into Cisco IOS Release 12.2(28)S.
12.2(31)SB	This command was integrated into Cisco IOS Release 12.2(31)SB.
12.2(33)SRB1	This command was integrated into Cisco IOS Release 12.2(33)SRB1.
12.2(33)SRC	This command was integrated into Cisco IOS Release 12.2(33)SRC.
15.2(2)SNI	This command was implemented on the Cisco ASR 901 Series Aggregation Services Routers.

Usage Guidelines

This command allows the MRRU value to be configured on MLP interfaces and member links. This command is useful for interfaces running an application such as IP Security (IPsec), where the addition of the IPsec header causes the packet to exceed the 1500-byte MTU of a typical IP packet.

When using a large-bundle interface MTU size, you must ensure that the individual frames-per-fragment size passed to the link interfaces is not greater than the link interface MTU setting or the peer MRRU setting. This size limit can be achieved in one of the following two ways:

- Configure the link interface MTU setting appropriately.
- Configure fragmentation such that the link MTU settings will never be violated.

When MLP is configured, several physical interfaces can constitute one logical connection to the peer. To represent the logical connection, software provides a logical interface, often called the bundle interface. This interface will have the IP address, for instance, and the MTU setting of the interface that IP uses when it is deciding whether to fragment an IP datagram that needs to be forwarded. The physical interfaces forward individual MLP fragments or frames that are given to them by the bundle interface.

The result of having to decide whether to fragment a packet is that, whereas with simple PPP the interface MTU must not exceed the peer's MRRU, with MLP the MTU size of the bundle interface must not exceed the MRRU setting of the peer.

The MRRU settings on both sides need not be equal, but the "must not exceed" rule just specified must be followed; otherwise a system might send several fragments that, when reconstructed as a frame, will be too large for the peer's receive buffer.

Once you configure the MRRU on the bundle interface, you enable the router to receive large reconstructed MLP frames. You may want to configure the bundle MTU so that the router can send large MLP frames, although it is not strictly necessary. The maximum recommended value for the bundle MTU is the value of the peer's MTU. The software will automatically reduce the bundle interface MTU if necessary to avoid violating the peer's MRRU.

When the bundle interface MTU is tuned to a higher number, then depending upon the fragmentation configuration, the link interface may be given larger frames to send. There are two possible solutions to this problem, as follows:

- Ensure that fragmentation is performed such that fragments are sized less than the link interface MTU (refer to the command pages for the **pppmultilinkfragmentdisable** and **pppmultilinkfragmentdelay** commands for more information about packet fragments).
- Configure the MTUs of the link interfaces such that they can send the larger frames.

Note Be careful when configuring MLP MRRU negotiation in a virtual private dialup network (VPDN) environment when an L2TP network server (LNS) is not running Cisco IOS Release 12.3(7)T. The software performs strict matching on the MRRU values in earlier versions of Cisco IOS software.

Examples

The following example shows how to configure MRRU negotiation on a virtual template with synchronous serial interfaces. The example also applies to asynchronous serial interfaces.

```
multilink virtual-template 1
!
interface virtual-template 1
 ip address 10.13.1.1 255.255.255.0
 mtu 1600
!
interface serial 0/0
 ppp multilink
 ppp multilink mrru local 1600
 mtu 1600
!
interface serial 0/1
 ppp multilink
 ppp multilink mrru local 1600
```

mtu 1600

The following example shows how to configure MRRU negotiation on multilink groups:

```
interface multilink 10
 ip address 10.13.1.1 255.255.255.0
 ppp multilink mrru local 1600
 mtu 1600
!
interface serial 0/0
 ppp multilink
 multilink-group 10
 mtu 1600
!
interface serial 0/1
 ppp multilink
 multilink-group 10
 mtu 1600
```

The following example shows how to configure MRRU negotiation on dialer interfaces:



Note Dialer interfaces are not supported on the Cisco 7600 series router.

```
interface dialer 1
 ip address 10.13.1.1 255.255.255.0
 encapsulation ppp
 dialer remote-name 2610-2
 dialer idle-timeout 30 inbound
 dialer string 5550101
 dialer pool 1
 dialer-group 1
 no cdp enable
 ppp multilink
 ppp multilink mrru local 1600
```

Related Commands

Command	Description
encapsulation ppp	Sets the PPP encapsulation method.
interface dialer	Defines a dialer rotary group.
mtu	Adjusts the maximum packet size or MTU size.
multilink virtual-template	Specifies a virtual template from which the specified MLP bundle interface can clone its interface parameters.
ppp multilink	Enables MLP on an interface.
ppp multilink fragment delay	Specifies a maximum time for the transmission of a packet fragment on an MLP bundle.
ppp multilink fragment disable	Disables packet fragmentation.
ppp multilink fragmentation	Sets the maximum number of fragments a packet will be segmented into before being sent over the bundle.

Command	Description
ppp multilink group	Restricts a physical link to joining only a designated multilink-group interface.
ppp multilink interleave	Enables MLP interleaving.

pri-group

To specify ISDN PRI on a channelized E1 or T1 card on a Cisco 7500 series router, use the **pri-group** command in controller configuration mode. To remove the ISDN PRI, use the **no** form of this command.

pri-group commandpri-group [**timeslots** *range*]
no pri-group

Syntax Description

timeslots *range*	(Optional) Specifies a single range of values from 1 to 23.

Command Default

Disabled

Command Modes

Controller configuration

Command History

Release	Modification
11.0	This command was introduced.
12.2(13)T	This command is no longer supported in Cisco IOS Mainline or Technology-based releases. It may conintue to appear in Cisco IOS 12.2S-family releases.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

When you configure ISDN PRI, you must first specify an ISDN switch type for PRI and an E1 or T1 controller.

Examples

The following example specifies ISDN PRI on T1 slot 1, port 0:

```
Router# isdn switch-type primary-4ess
Router(config)# controllers t1 1/0
Router(config-controller)# framing esf
Router(config-controller)# linecode b8zs
Router(config-controller)# pri-group timeslots 2-6
```

Related Commands

Command	Description
controller	Configures a T1 or E1 controller and enters controller configuration mode.
interface serial	Specifies a serial interface created on a channelized E1 or channelized T1 controller (for ISDN PRI, CAS, or robbed-bit signaling).
isdn switch-type (PRI)	Specifies the central office switch type on the ISDN PRI interface.

priority1

To set a preference level for a Precision Time Protocol clock, use the **priority1** command in PTP clock configuration mode. To remove a priority1 configuration, use the **no** form of this command.

priority1 *priorityvalue*
no priority1 *priorityvalue*

Syntax Description

priorityvalue	Number value of the preference level. The range is from 0 to 255; lower values indicate a higher precedence. The default value is 128.

Command Default

The default preference level is 128.

Command Modes

PTP clock configuration (config-ptp-clk)

Command History

Release	Modification
15.0(1)S	This command was introduced.
15.1(2)SNG	This command was implemented on the Cisco ASR 901 Series Aggregation Services Router.

Usage Guidelines

Subordinate devices use the priority1 value when selecting a primary clock. The priority1 value has precedence over the priority2 value.

Examples

The following example shows how to configure a ptp priority1 value:

```
Device> enable
Device# configure terminal
Device# ptp clock ordinary domain 0
Device(config-ptp-clk)# priority1 128
Device(config-ptp-clk)# end
```

Related Commands

Command	Description
priority2	Sets the PTP priority2 value.

priority2

To set a set a secondary preference level for a Precision Time Protocol clock, use the **priority2** command in PTP clock configuration mode. To remove a priority2 configuration, use the **no** form of this command.

priority2 *priorityvalue*
no priority2 *priorityvalue*

Syntax Description

priorityvalue	The number value of the preference level. The range is from 0 to 255; lower values indicate a higher precedence. The default value is 128.

Command Default

The default preference level is 128.

Command Modes

PTP clock configuration (config-ptp-clk)

Command History

Release	Modification
15.0(1)S	This command was introduced.
15.1(2)SNG	This command was implemented on the Cisco ASR 901 Series Aggregation Services Router.

Usage Guidelines

Subordinate devices use the priority2 value to select a primary clock; the priority2 value is only considered when the device cannot use priority1 and other clock attributes to select a clock.

Examples

The following example shows how to configure the ptp priority2 value:

```
Device> enable
Device# configure terminal
Device# ptp clock ordinary domain 0
Device(config-ptp-clk)# priority2 128
Device(config-ptp-clk)# end
```

Related Commands

Command	Description
priority1	Sets the PTP priority1 value.

proactive enable

To enable automatic triggering of Forward Error Correction-Fast Re-Route (FEC-FRR), use the **proactive enable** command in DWDM configuration mode. To disable automatic triggering, use the no form of this command.

proactive enable

This command has no arguments or keywords.

Command Modes

DWDM Controller (config-controller)

Command History

Release	Modification
15.2(1)S	This command was introduced on the Cisco 7600 series routers.

Usage Guidelines

Examples

This example shows how to enable automatic triggering of Forward Error Correction-Fast Re-Route (FEC-FRR):

```
Router# configure terminal
Router(config)# controller dwdm 0/1
Router(config-controller)# proactive enable
```

Related Commands

Command	Description
proactive trig-threshold	Configures the trigger threshold of Forward Error Correction-Fast Re-Route (FEC-FRR).
proactive trig-window	Configures the trigger window (in milliseconds) in which Fast Re-Route may be triggered.
proactive rvrt-threshold	Configures the revert threshold to trigger reverting from the Forward Error Correction-Fast Re-Route (FEC-FRR) route back to the original route.
proactive rvrt-window	Configures the revert window in which reverting from the Forward Error Correction-Fast Re-Route (FEC-FRR) route back to the original route is triggered.

proactive rvrt-threshold

To configure the revert threshold to trigger reverting from the Forward Error Correction-Fast Re-Route (FEC-FRR) route back to the original route, use the **proactive rvrt-threshold** command in DWDM configuration mode. To remove the revert threshold, use the **no** form of this command.

proactive rvrt-threshold *x-coeff y-power*
no proactive rvrt-threshold *x-coeff y-power*

Syntax Description

x-coeff	Bit error rate coefficient (x of xE-y). The range is 1 to 9.
y-power	Bit error rate exponent (y of xE-y). The range is 3 to 9.

Command Default

Standard FEC mode: 1E-5

Enhanced FEC Mode: 1E-4

Command Modes

DWDM Controller (config-controller)

Command History

Release	Modification
15.2(1)S	This command was introduced on the Cisco 7600 series routers.

Examples

This example shows how to configure the revert threshold for FEC-FRR:

```
Router>enable
Router# configure terminal
Ruter(config)# controller dwdm 0/1
Router(config-controller)# proactive rvrt-threshold 1 6
```

Related Commands

Command	Description
proactive enable	Enables automatic triggering of Forward Error Correction-Fast Re-Route (FEC-FRR).
proactive trig-threshold	Configures the trigger threshold of Forward Error Correction-Fast Re-Route (FEC-FRR).
proactive trig-window	Configures the trigger window in which Fast Re-Route may be triggered.
proactive rvrt-window	Configures the revert window in which reverting from the Forward Error Correction-Fast Re-Route (FEC-FRR) route back to the original route is triggered.

proactive rvrt-window

To configure the revert window in which reverting from the Forward Error Correction-Fast Re-Route (FEC-FRR) route back to the original route is triggered, use the **proactive rvrt-window** command in DWDM configuration mode. To remove the revert window, use the no form of this command.

proactive rvrt-window *window*
no proactive rvrt-window *window*

Syntax Description

window	The length of time (in milliseconds) of the window in which reverting from FEC-FRR may be triggered. The range is 2000 to 100000.

Command Default

The default value of time is 2000.

Command Modes

DWDM configuration (config-controller)

Command History

Release	Modification
15.2(1)S	This command was introduced on the Cisco 7600 series routers.

Examples

This example shows how to configure the window in which reverting from FEC-FRR may be triggered:

```
Router# configure terminal
Router(config)# controller dwdm 0/1
Router(config-controller)# proactive rvrt-window 20345
```

Related Commands

Command	Description
proactive enable	Enables automatic triggering of Forward Error Correction-Fast Re-Route (FEC-FRR).
proactive trig-threshold	Configures the trigger threshold of Forward Error Correction-Fast Re-Route (FEC-FRR).
proactive trig-window	Configures the trigger window (in milliseconds) in which Fast Re-Route may be triggered.
proactive rvrt-threshold	Configures the revert threshold to trigger reverting from the Forward Error Correction-Fast Re-Route (FEC-FRR) route back to the original route.

proactive trig-threshold

To configure the trigger threshold of Forward Error Correction-Fast Re-Route (FEC-FRR), use the **proactive trig-threshold** command in DWDM configuration mode. To remove the trigger threshold, use the**no** form of this command.

proactive trig-threshold *x-coeff y-power*
no proactive trig-threshold *x-coeff y-power*

Syntax Description

x-coeff	Bit error rate coefficient (x of xE-y). The range is 1 to 9. Default is 1.
y-power	Bit error rate exponent (y of xE-y). The range is 3 to 9.

Command Default

Standard FEC mode: 6E-5

Enhanced FEC Mode: 6E-4

Command Modes

DWDM Controller (config-controller)

Command History

Release	Modification
15.2(1)S	This command was introduced on the Cisco 7600 series routers.

Examples

This example shows how to configure the trigger threshold of Forward Error Correction-Fast Re-Route (FEC-FRR).

```
Router# configure terminal
Router(config)# controller dwdm 0/1
Router(config-controller)#proactive trig-threshold 1 9
```

Related Commands

Command	Description
proactive enable	Enables automatic triggering of Forward Error Correction-Fast Re-Route (FEC-FRR).
proactive trig-window	Configures the trigger window (in milliseconds) in which Fast Re-Route may be triggered.
proactive rvrt-threshold	Configures the revert threshold to trigger reverting from the Forward Error Correction-Fast Re-Route (FEC-FRR) route back to the original route.

Command	Description
proactive rvrt-window	Configures the revert window in which reverting from the Forward Error Correction-Fast Re-Route (FEC-FRR) route back to the original route is triggered.

protection-group

Use this command to configure virtual protection group interface.

protection-group *group id type STS48c*

Syntax Description

Syntax Description:

group id	Identifier for the interface that is created
type	Protection group type It can be STS, STS3c, STS12c, and STS48c

Command Default

None

Command Modes

Controller configuration

Command History

Release	Modification
Cisco IOS XE Everest 16.5.1	Support for this command was introduced for the Cisco NCS 4200 Series and Cisco ASR 900 Series Routers.

Usage Guidelines

This command is used for configuring protection group parameters.

Examples

The following example shows how to configure protection group:

```
enable
configure terminal
protection-group 401 type STS48c
controller protection group 401
type STS48c
cem-group 19001 cep
end
```

Related Commands

Command	Description
show protection-group	Verifies the protection group configuration.

protection-group [working | protect]

Use this command to configure protection group roles.

protection-group *group id* [**working** | **protect**]

Syntax Description

Syntax Description:

group id	Identifier for the interface that is created
working	The working interface for protection group
protect	The protect interface for protection group

Command Default

None

Command Modes

Controller configuration

Command History

Release	Modification
Cisco IOS XE Everest 16.5.1	Support for this command was introduced for the Cisco NCS 4200 Series and Cisco ASR 900 Series Routers.

Usage Guidelines

Define the role either working interface or protect interface in the protection group.

Examples

The following example shows how to configure UPSR work path protection:

```
enable
configure terminal
controller mediatype 0/3/6
mode sonet
controller sonet 0/3/6
rate oc48
sts-1 1-48 mode sts-48c
protection-group 401 working
end
```

Related Commands

Command	Description
show protection-group	Verifies the protection group configuration.

protocol gre

To specify GRE as the tunnel mode and to set the GRE key for configuring the L3VPN encapsulation profile, use the **protocolgre** command in L3 VPN encapsulation configuration mode. To remove the transport source, use the **no** form of this command.

protocol gre [**key** *gre key*]
no protocol [**gre**]

Syntax Description

key	(Optional) Specifies the key for GRE tunnel interface.
gre key	(Optional) The GRE key value. The range is from 0 to 4294967295.

Command Default

The tunnel mode and GRE key are not specified.

Command Modes

L3VPN Encapsulation Configuration (config-l3vpn-encap-ip)

Command History

Release	Modification
12.2(33)SRE	This command was introduced.

Examples

The following example shows how to specify GRE as the tunnel mode and to set the GRE key:

```
Router(config-l3vpn-encap-ip)# protocol gre key 500
```

Related Commands

Command	Description
l3vpn encapsulation ip	Configures the L3VPN encapsulation profile.
transport ipv4	Specifies IPv4 transport source mode and the transport source interface.
show l3vpn encapsulation ip	Displays the profile health and the underlying tunnel interface.

ptp clock

To create a Precision Time Protocol clock and specify the clock mode, use the **ptpclock** command in the global configuration mode. To remove a ptp clock configuration, use the **no** form of this command.

ptp clock {**ordinary** | **transparent**} **boundary domain** *domain*
no ptp clock {**ordinary** | **transparent**} **boundary domain** *domain*

Syntax Description

ordinary	Sets the PTP clock to ordinary clocking mode.
transparent	Sets the PTP clock to transparent clock mode; the router modifies outgoing PTP sync and delay-request messages to account for residence time using the correction field in the follow-up message.
boundary	Sets the PTP clock to boundary clock mode; the router participates in selecting the best master clock and can act as the master clock if no better clocks are detected.
domain	The PTP clocking domain number. Valid values are from 0 to 127.

Command Default

No default behavior or values.

Command Modes

Global configuration (config)

Command History

Release	Modification
15.0(1)S	This command was introduced.

Usage Guidelines

This command creates a new PTP clock and enters clock configuration mode.

Examples

The following example shows how to configure a PTP clock and enter clock configuration mode:

```
Router# configure terminal
Router# ptp clock ordinary domain 0
Router(config-ptp-clk)#
```

Related Commands

Command	Description
clock-port	Specifies the mode of a PTP clock port.

pulse-time

To enable pulsing data terminal ready (DTR) signal intervals on the serial interfaces, use the **pulse-time** command in interface configuration mode. To restore the default interval, use the **no** form of this command.

pulse-time[**msec***seconds*]
no pulse-time

Syntax Description

msec	(Optional) Specifies the use of milliseconds for the DTR signal interval.
seconds	Integer that specifies the DTR signal interval in seconds. If the **msec** keyword is configured, the DTR signal interval is specified in milliseconds. The default is 0.

Command Default

0 seconds

Command Modes

Interface configuration

Command History

Release	Modification
10.0	This command was introduced.
12.1(5)T	The optional **msec** keyword was added to configure the interval in milliseconds.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

When the serial line protocol goes down (for example, because of loss of synchronization), the interface hardware is reset and the DTR signal is held inactive for at least the specified interval. This function is useful for handling encrypting or other similar devices that use the toggling of the DTR signal to resynchronize.

Use the optional **msec** keyword to specify the DTR signal interval in milliseconds. A signal interval set to milliseconds is recommended on High-Speed Serial Interfaces (HSSIs).



Note Whenever the **pulse-time** command is configured for the synchronous serial interface, do one of the following after every interface state transition. This ensures that the DTR is pulsed down for the configured interval:

- In exec mode, issue the **clear interface serial** *x*/*y*/[*z*] command.
- In config mode of the serial interface, issue a **shutdown**, followed by **no shutdown**.

If you do not clear/reset the interface with one of these procedures, the **pulse-time** command will have no effect.

Optionally, you can automate this procedure using an EEM or Tcl script. The following example EEM script clears the serial interface after a disconnection:

```
event manager applet CLEAR_INIT_S000
 event syslog pattern "Line protocol on Interface Serial0/0/0, changed state to down"
 action 2.0 cli command "enable"
 action 2.1 cli command "clear int Serial0/0/0"
 action 3.0 syslog msg "clear int Serial0/0/0"
```

Examples

The following example enables DTR pulse signals for 3 seconds on serial interface 2:

```
Router(config)# interface serial 2
Router(config-if)# pulse-time 3
```

The following example enables DTR pulse signals for 150 milliseconds on HSSI interface 2/1/0:

```
Router(config)# interface hssi 2/1/0
Router(config-if)# pulse-time msec 150
```

rate

Use this command to enable the rate for SONET and SDH ports.

For SONET:

rate [*OC3* | *OC12* | *OC48* | *OC192*

For SDH:

rate [*STM-1* | *STM-4* | *STM-16* | *STM-64*

Syntax Description

Syntax Description:

OC3	Configures OC-3 port.
OC12	Configures OC-12 port.
OC-48	Configures OC-48 port.
OC-192	Configures OC-192 port.
STM-1	Configures STM-1 port.
STM-4	Configures STM-4 port.
STM-16	Configures STM-16 port.
STM-64	Configures STM-64 port.

Command Default

None

Command Modes

Controller configuration

Command History

Release	Modification
XE 3.18SP	Support for this command was introduced on NCS 4200 Series for SONET.
XE Everest 16.6.1	This command was integrated into the Cisco NCS 4200 Series and Cisco ASR 900 Series for SDH.

Usage Guidelines

Configuration of this command is mandatory.

Examples

The following example shows how to configure Mediatype controller mode:

```
enable
configure terminal
controller MediaType 0/5/0
mode sonet
controller sonet 0/5/0
rate oc3
end
```

To configure mode VC4 CEP:

```
enable
configure terminal
controller sdh 0/5/0
rate stm 4
aug mapping au-4
au-4 1
mode vc4
cem-group 100 cep
end
```

Related Commands

Command	Description
controller sonet	Configures the SONET mode.
show controller sonet	Displays SONET controller configuration.

recovered-clock

To configure an associated clock ID with the corresponding CEM circuit, use the **recovered-clock** command in global configuration mode.

recovered-clock *bay slot*

Syntax Description

bay	Identifies the bay where the CEM circuit is inserted. On NCS4200 series bay value is 0 always.
slot	Physical slot number. The slot number is in a range either from 0 to 5 or 8 to 13, depending on the slot in which the STM-1 card resides. The slot is always 0 for Cisco NCS 4200 Series. The physical slot ranges from 0 to 5 for Cisco ASR 900 Series Routers. The value of physical slot supported for Cisco ASR 920 Routers is 1.

Command Default

None

Command Modes

Global configuration

Command History

Release	Modification
XE 3.18SP	This command was integrated into Cisco NCS 4200 Series
XE Everest 16.5.1	This command was integrated into Cisco NCS 4200 Series. This command was introduced into Cisco ASR 900 Series routers.

Usage Guidelines

This command will be used when the clock needs to be recovered by the same CEM circuit.

The following example shows how to configure an associated clock ID with the corresponding CEM circuit.

```
recovered-clock 0 3
 clock recovered 1 differential cem 0 1
```

Related Commands

Command	Description
clock recovered adaptive/differential cem	Associates the clock recovered ID to the CEM group.

redundancy

To enter redundancy configuration mode, use the **redundancy**command in global configuration mode. This command does not have a **no** form.

redundancy

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

Global configuration (config)

Command History

Release	Modification
12.1(5)XV1	This command was introduced on the Cisco AS5800 universal access server.
12.2(4)XF	This command was introduced for the Cisco uBR10012 router.
12.2(11)T	This command was integrated into Cisco IOS Release 12.2(11)T.
12.0(9)SL	This command was integrated into Cisco IOS Release 12.0(9)SL.
12.0(16)ST	This command was implemented on the Cisco 7500 series Internet routers.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(14)SX	Support for this command was added for the Supervisor Engine 720.
12.2(18)S	This command was implemented on the Cisco 7500 series Internet routers.
12.2(20)S	This command was implemented on the Cisco 7304 router.
12.2(17d)SXB	Support for this command on the Supervisor Engine 2 was extended to Release 12.2(17d)SXB.
12.3(7)T	This command was implemented on the Cisco 7500 series Internet routers.
12.2(8)MC2	This command was implemented on the MWR 1900 Mobile Wireless Edge Router (MWR).
12.3(11)T	This command was implemented on the MWR 1900 MWR.
12.3BC	This command was integrated into Cisco IOS Release 12.3BC.
12.0(22)S	This command was implemented on the Cisco 10000 series Internet routers.
12.2(18)SXE2	This command was integrated into Cisco IOS Release 12.2(18)SXE2.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(44)SQ	This command was integrated into Cisco IOS Release 12.2(44)SQ. Support for the Cisco RF Gateway 10 was added.

Release	Modification
12.2(33) SRE	This command was modified. The interchassis subconfiguration mode was added.

Usage Guidelines

Use the **redundancy** command to enter redundancy configuration mode, where you can define aspects of redundancy such as shelf redundancy for the Cisco AS5800 universal access server.

Cisco 10000 Series Router

Before configuring line card redundancy, install the Y-cables. Before deconfiguring redundancy, remove the Y-cables.

The following restrictions apply to line card redundancy on the Cisco 10000 series router:

- Port-level redundancy is not supported.
- Redundant cards must occupy the two subslots within the same physical line card slot.
- The line card that will act as the primary line card must be the first line card configured, and it must occupy subslot 1.

Cisco 7600 Series Router

From redundancy configuration mode, you can enter the main CPU submode to manually synchronize the configurations that are used by the two supervisor engines.

From the main CPU submode, you can use the **auto-sync** command to use all the redundancy commands that are applicable to the main CPU.

To select the type of redundancy mode, use the **mode** command.

Nonstop forwarding (NSF) with stateful switchover (SSO) redundancy mode supports IPv4. NSF with SSO redundancy mode does not support IPv6, Internetwork Packet Exchange (IPX), and Multiprotocol Label Switching (MPLS).

After you enter redundancy configuration mode, you can use the **interchassis** command to specify the redundancy group number and enter interchassis redundancy mode. In the interchassis redundancy configuration mode, you can do the following:

- Specify a backbone interface for the redundancy group using the **backbone** command.
- Exit from interchassis configuration mode using the **exit** command.
- Specify the IP address of the remote redundancy group member using the **member ip** command.
- Specify the multichassis LACP (mLACP) node ID, system MAC address, and system priority using the **node-id**, **system-mac**, and **system-priority** commands.
- Define the peer monitoring method using the **monitor** command.

Cisco uBR10012 Universal Broadband Router

After you enter redundancy configuration mode, you can use the **main-cpu** command to enter main-CPU redundancy configuration mode, which allows you to specify which files are synchronized between the active and standby Performance Routing Engine (PRE) modules.

Cisco RF Gateway 10

At the redundancy configuration mode, you can do the following:

- Set a command to its default mode using the **default** command.
- Exit from a redundancy configuration using the **exit** command.
- Enter the line card group redundancy configuration using the **linecard-group** command.
- Enter main-CPU redundancy configuration mode using the **main-cpu** command, which allows you to specify which files are synchronized between the active and standby Supervisor cards.
- Configure the redundancy mode for the chassis using the **mode** command.
- Enforce a redundancy policy using the **policy** command.

Examples

The following example shows how to enable redundancy mode:

```
Router(config)# redundancy
Router(config-red)#
```

The following example shows how to assign the configured router shelf to the redundancy pair designated as 25. This command must be issued on both router shelves in the redundant router-shelf pair:

```
Router(config)# redundancy
Router(config-red)# failover group-number 25
```

Cisco 10000 Series Router

The following example shows how to configure two 4-port channelized T3 half eight line cards that are installed in line card slot 2 for one-to-one redundancy:

```
Router(config)# redundancy
Router(config-r)# linecard-group 1 y-cable
Router(config-r-lc)# member subslot 2/1 primary
Router(config-r-lc)# member subslot 2/0 secondary
```

Cisco 7600 Series Router

The following example shows how to enter the main CPU submode:

```
Router(config)#
redundancy
Router(config-r)#
main-cpu
Router(config-r-mc)#
```

Cisco uBR10012 Universal Broadband Router

The following example shows how to enter redundancy configuration mode and display the commands that are available in that mode on the Cisco uBR10012 router:

```
Router# configure terminal
```

```
Router(config)# redundancy

Router(config-r)# ?

Redundancy configuration commands:
  associate  Associate redundant slots
  exit       Exit from redundancy configuration mode
  main-cpu   Enter main-cpu mode
  no         Negate a command or set its defaults
```

The following example shows how to enter redundancy configuration mode and displays its associated commands on the Cisco RFGW-10 chassis:

```
Router# configure terminal
Router(config)# redundancy
Router(config-r)#?
Redundancy configuration commands:
  default         Set a command to its defaults
  exit            Exit from redundancy configuration mode
  linecard-group  Enter linecard redundancy submode
  main-cpu        Enter main-cpu mode
  mode            redundancy mode for this chassis
  no              Negate a command or set its defaults
  policy          redundancy policy enforcement
```

The following example shows how to enter redundancy configuration mode and its associated commands in the interchassis mode:

```
Router# configure terminal
Router(config)# redundancy
```

Router(config-r)#?

```
Redundancy configuration commands:
  exit          Exit from redundancy configuration mode
  interchassis  Enter interchassis mode
  no            Negate a command or set its defaults
Router(config-r)# interchassis group 100

R1(config-r-ic)# ?
Interchassis redundancy configuration commands:
  backbone  specify a backbone interface for the redundancy group
  exit      Exit from interchassis configuration mode
  member    specify a redundancy group member
  mlacp     mLACP interchassis redundancy group subcommands
  monitor   define the peer monitoring method
  no        Negate a command or set its defaults
```

Related Commands

Command	Description
associate slot	Logically associates slots for APS processor redundancy.
auto-sync	Enables automatic synchronization of the configuration files in NVRAM.
clear redundancy history	Clears the redundancy event history log.
linecard-group y-cable	Creates a line card group for one-to-one line card redundancy.

Command	Description
main-cpu	Enters main-CPU redundancy configuration mode for synchronization of the active and standby PRE modules or Supervisor cards.
member subslot	Configures the redundancy role of a line card.
mode (redundancy)	Configures the redundancy mode of operation.
redundancy force-switchover	Switches control of a router from the active RP to the standby RP.
show redundancy	Displays information about the current redundant configuration and recent changes in states or displays current or historical status and related information on planned or logged handovers. In the redundancy configuration of Cisco ASR 920 Series Routers, the commands related to MR-APS feature are only supported.

redundancy all-active replicate

To enable all-active pseudowire redundancy mode with traffic replication, use the **redundancy all-active replicate** command in global or interface configuration mode. To disable this functionality, use the **no** form of this command.

redundancy all-activereplicate
no redundancy all-activereplicate

Syntax Description

replicate	Replicates the pseudowire state on the router.

Command Default

No default behavior or values.

Command Modes

Global configuration (config)

Interface configuration (config-if)

Command History

Release	Modification
Cisco IOS XE Release 3.18.1SP	This command was introduced on the Cisco ASR 900 Series Routers.

Usage Guidelines

The **redundancy all-active replicate** command maintains the working ad protect pseudowires in a pseudowire redundancy configuration with MR-APS configuration to remain in the UP state.

Examples

The following example shows the configuration at global level:

```
pseudowire-class 2G-PW
encapsulation mpls
status peer topology dual-homed

controller E1 0/1
framing unframed
cem-group 8 unframed
```

The following examples shows the configuration at interface level:

```
interface CEM0/1
no ip address
cem 8
xconnect 10.10.10.1 8 encapsulation mpls pw-class 2G-PW
backup peer 10.10.10.2 8 pw-class 2G-PW
redundancy all-active replicate
```

Related Commands

Command	Description
pseudowire class	Configures the pseudowire class on the router.
template typepseudowire	Configures the pseudowire template on the router.

redundancy force-switchover

To force the standby Route Processor (RP) or Supervisor card to assume the role of the active RP or Supervisor card, use the **redundancy force-switchover** command in privileged EXEC mode.

redundancy force-switchover [**main-cpu**]

Syntax Description

main-cpu	(Optional) Forces switchover to the main CPU.

Command Default

No default behavior or values.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.0(16)ST	This command was introduced.
12.1(10)EX2	This command was integrated into Cisco IOS Release 12.1(10)EX2.
12.0(17)ST	This command was implemented on the Cisco 12000 series routers.
12.0(22)S	This command replaces the **force-failover**command on the Cisco 10000 series routers.
12.2(14)SX	Support for this command was added for the Supervisor Engine 720.
12.2(18)S	This command was implemented on the Cisco 7500 series routers.
12.2(20)S	Support was added for the Cisco 7304 router.
12.3(7)T	This command was integrated into Cisco IOS Release 12.3(7)T.
12.2(17d)SXB	Support for this command on the Supervisor Engine 2 was extended to Cisco IOS Release 12.2(17d)SXB.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SCA	This command was integrated into Cisco IOS Release 12.2(33)SCA.
12.2(44)SQ	This command was integrated into Cisco IOS Release 12.2(44)SQ. Support for the Cisco RF Gateway 10 was added.

Usage Guidelines

Use the **redundancy force-switchover** command to switch control of a router from the active RP or Supervisor card to the standby RP or Supervisor card. Both the active and standby RPs or Supervisor cards must have a high availability Cisco IOS image installed and must be configured for Route Processor Redundancy (RPR) mode before the **redundancy force-switchover** command can be used. Before the system switches over, it verifies that the standby RP or Supervisor card is ready to take over.

When you use the **redundancy force-switchover**command and the current running configuration is different from the startup configuration, the system prompts you to save the running configuration before the switchover is performed.

Note All line cards will reset in RPR mode on a switchover.

Note Before using this command in Cisco 7600 series routers, refer to the "Performing a Fast Software Upgrade" section of the *Cisco 7600 Series Router Cisco IOS Software Configuration Guid*e for additional information.

On Cisco 7600 series routers, the **redundancy force-switchover** command conducts a manual switchover to the redundant supervisor engine. The redundant supervisor engine becomes the new active supervisor engine running the new Cisco IOS image. The modules are reset and the module software is downloaded from the new active supervisor engine.

The active and redundant supervisor engines do not reset on a Route Processor Redundancy Plus (RPR+) switchover. The old active supervisor engine reboots with the new image and becomes the redundant supervisor engine.

Beginning with Cisco IOS Release 12.2(33)SCA, you can force a Performance Routing Engine (PRE) switchover using the **redundancy force-switchover main-cpu** command from either the primary or standby PRE. If you force a switchover from the active PRE, both PREs synchronize and the active PRE reloads normally. When you force a switchover from the standby PRE, a crash dump of the active PRE occurs for troubleshooting purposes. Forcing a switchover from the standby PRE should only be done if you cannot access the active PRE.

Examples

The following example shows a switchover from the active RP to the standby RP on a Cisco 7513 router with RPR configured:

```
Router# configure terminal
Router(config)# hw-module slot 7 image slot0:rsp-pv-mz
Router(config)# hw-module slot 6 image slot0:rsp-pv-mz
Router(config)# slave auto-sync config
Router(config)# redundancy
Router(config-r)# mode rpr
Router(config-r)# end
Router# copy running-config startup-config
Router# redundancy force-switchover
```

The following example shows how to perform a manual switchover from the active to the standby RP when the running configuration is different from the startup configuration:

```
Router# redundancy force-switchover
System configuration has been modified. Save? [yes/no]:y
Building configuration...
...
...
[OK]
Proceed with switchover to standby NSE? [confirm]y
00:07:35:%SYS-5-SWITCHOVER:Switchover requested
```

The following example shows how to perform a manual switchover from the active to the standby RP when the running configuration is the same as the startup configuration:

```
Router# redundancy force-switchover
Proceed with switchover to standby NSE? [confirm]
00:07:35:%SYS-5-SWITCHOVER:Switchover requested
```

Cisco RF Gateway 10

The following example shows how to perform a manual switchover from the active to the standby RP when the running configuration is different from the startup configuration:

```
Router# redundancy force-switchover
System configuration has been modified. Save? [yes/no]:y
Building configuration...
...
...
[OK]
Proceed with switchover to standby NSE? [confirm]y
00:07:35:%SYS-5-SWITCHOVER:Switchover requested
```

The following example shows how to perform a manual switchover from the active to the standby RP when the running configuration is the same as the startup configuration:

```
Router# redundancy force-switchover
Proceed with switchover to standby NSE? [confirm]
00:07:35:%SYS-5-SWITCHOVER:Switchover requested
```

Related Commands

Command	Description
clear redundancy history	Clears the redundancy event history log.
hw-module sec-cpu reset	Resets and reloads the standby RP with the specified Cisco IOS image and executes the image.
hw-module slot image	Specifies a high availability Cisco IOS image to run on an active or standby RP.
mode (HSA redundancy)	Configures the High System Availability (HSA) redundancy mode.
mode (redundancy)	Configures the redundancy mode of operation.
redundancy	Enters redundancy configuration mode.
show redundancy	Displays current active and standby Performance Routing Engine (PRE) redundancy status.

redundancy handover

To hand over control of resources (slots and cards) from a route-switch-controller (RSC) card to its peer RSC card, use the **redundancyhandover** command in privileged EXEC mode.

redundancy handover {**cancel** | {**peer-resources** | **shelf-resources**} [**busyout-period** *mins*] [**at** *hh* **:** *mm* [{*day month* | *month day*} *year*]]}

Syntax Description

cancel	Any pending handover is canceled.
peer-resources	Resources to be handed over are those on the side of the peer RSC. This parameter applies only when the system is in extraload.
shelf-resources	Resources to be handed over are those on the side of the RSC from which the command is run.
busyout-period *mins*	(Optional) Time period for which all slots in the selected resources are to be busied out before handover. If time options are omitted, handover or busyout period begins immediately.
at *hh* **:** *mm day month year*	(Optional) Time of the handover or start of the busyout period, in 24-hour time format; hour and minute are required; day, month, and year are optional.

Command Default

Control remains with the assigned RSC.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(2)XB1	This command was introduced.
12.2(11)T	This command was integrated into Cisco IOS Release 12.2(11)T.

Usage Guidelines

To use this command, you must have two RSC cards installed on your Cisco AS5850 and you must be connected to one of them in handover-split mode. This command can be run from either RSC and can specify that slots be handed over to the peer RSC.

After handover and subsequent restoration of the failed RSC, connect to the active RSC and use this command to return control of cards to the previously failed but now restored RSC.

Note that when you enter the command with the **shelf-resources** option, the RSC reloads.

Examples

The following example hands over control, to the peer RSC, of the slots and cards on the corresponding side of the chassis. Note the prompt to confirm clearing of calls, handover, and reload on the last line.

```
Router# redundancy handover shelf-resources busyout-period 10 at 22:00 3 Sep 2005

Newly entered handover schedule:
Busyout period at 22:00:00 PDT Sat Sep 3 2005 for a duration of 10 minutes
```

```
Handover pending at 22:10:00 PDT Sat Sep 3 2005
Clear calls, handover and reload as specified above? y
```

Related Commands

Command	Description
show redundancy debug-log	Displays up to 256 relevant debug entries.
show redundancy handover	Displays details of any pending handover (that is, a handover command that was entered previously and is not yet completed).
show redundancy history	Displays logged handover events.

redundancy stateful

To configure stateful failover for tunnels using IP Security (IPSec), use the **redundancystateful**command in crypto map configuration mode. To disable stateful failover for tunnel protection, use the **no** form of this command.

redundancy *standby-group-name* **stateful**
no redundancy *standby-group-name* **stateful**

Syntax Description

standby-group-name	Refers to the name of the standby group as defined by Hot Standby Router Protocol (HSRP) standby commands. Both routers in the standby group are defined by this argument and share the same virtual IP (VIP) address.

Command Default

Stateful failover is not enabled for IPSec tunnels.

Command Modes

Crypto map configuration

Command History

Release	Modification
12.3(11)T	This command was introduced.

Usage Guidelines

The **redundancystateful**command uses an existing IPSec profile (which is specified via the **cryptoipsecprofile**command) to configure IPSec stateful failover for tunnel protection. (You do not configure the tunnel interface as you would with a crypto map configuration.) IPSec stateful failover enables you to define a backup IPSec peer (secondary) to take over the tasks of the active (primary) router if the active router is deemed unavailable.

The tunnel source address must be a VIP address, and it must not be an interface name.

Examples

The following example shows how to configure stateful failover for tunnel protection:

```
crypto ipsec profile peer-profile
  redundancy HA-out stateful

interface Tunnel1
 ip unnumbered Loopback0
 tunnel source 209.165.201.3
 tunnel destination 10.0.0.5
 tunnel protection ipsec profile peer-profile
!
interface Ethernet0/0
 ip address 209.165.201.1 255.255.255.224
 standby 1 ip 209.165.201.3
 standby 1 name HA-out
```

Related Commands

Command	Description
crypto ipsec profile	Defines the IPSec parameters that are to be used for IPSec encryption between two routers and enters crypto map configuration mode.

remote command

To execute a Cisco 7600 series router command directly on the switch console or a specified module without having to log into the Cisco 7600 series router first, use the **remote command** command in privileged EXEC mode.

remote command {**module** *num* | **standby-rp** | **switch**} *command*

Syntax Description

module *num*	Specifies the module to access; see the "Usage Guidelines" section for valid values.
standby-rp	Specifies the standby route processor.
switch	Specifies the active switch processor.
command	Command to be executed.

Command Default

This command has no default settings.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(14)SX	Support for this command was introduced on the Supervisor Engine 720.
12.2(17d)SXB	Support for this command on the Supervisor Engine 2 was extended to Release 12.2(17d)SXB.
12.2(18)SXD	The **standby-rp** keyword was added.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

The **module** *num* keyword and argument designate the module number. Valid values depend on the chassis that is used. For example, if you have a 13-slot chassis, valid values are from 1 to 13. The **module** *num* keyword and argument are supported on DFC-equipped modules and the standby supervisor engine only.

When you execute the **remote command switch**command, the prompt changes to Switch-sp#.

This command is supported on DFC-equipped modules and the supervisor engine only.

This command does not support command completion, but you can use shortened forms of the command (for example, entering **sh** for **show**).

Examples

This example shows how to execute the **show calendar** command from the standby route processor:

```
Router#
remote command standby-rp show calendar
Switch-sp#
09:52:50 UTC Mon Nov 12 2001
Router#
```

Related Commands

Command	Description
remote login	Accesses the Cisco 7600 series router console or a specific module.

remote-span

To configure a virtual local area network (VLAN) as a remote switched port analyzer (RSPAN) VLAN, use the **remote-span** command in config-VLAN mode. To remove the RSPAN designation, use the **no** form of this command.

remote-span
no remote-span

Syntax Description

This command has no arguments or keywords.

Command Default

This command has no default settings.

Command Modes

Config-VLAN mode

Command History

Release	Modification
12.2(14)SX	Support for this command was introduced on the Supervisor Engine 720.
12.2(17d)SXB	Support for this command on the Supervisor Engine 2 was extended to Release 12.2(17d)SXB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

This command is not supported in the VLAN database mode.

You can enter the **show vlan remote-span** command to display the RSPAN VLANs in the Cisco 7600 series router.

Examples

This example shows how to configure a VLAN as an RSPAN VLAN:

```
Router(config-vlan)# remote-span
Router(config-vlan)
```

This example shows how to remove the RSPAN designation:

```
Router(config-vlan)# no remote-span
Router(config-vlan)
```

Related Commands

Connect	Description
show vlan remote-span	Displays a list of RSPAN VLANs.

remote login

To access the Cisco 7600 series router console or a specific module, use the **remote login** command in privileged EXEC mode.

remote login {**module** *num* | **standby-rp** | **switch**}

Syntax Description

module *num*	Specifies the module to access; see the "Usage Guidelines" section for valid values.
standby-rp	Specifies the standby route processor.
switch	Specifies the active switch processor.

Command Default

This command has no default settings.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(14)SX	Support for this command was introduced on the Supervisor Engine 720.
12.2(17d)SXB	Support for this command on the Supervisor Engine 2 was extended to Release 12.2(17d)SXB.
12.2(18)SXD	This command was changed to include the **standby-rp** keyword.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines



Caution When you enter the **attach** or **remote login** command to access another console from your switch, if you enter global or interface configuration mode commands, the switch might reset.

The **module** *num* keyword and argument designate the module number. Valid values depend on the chassis that is used. For example, if you have a 13-slot chassis, valid values are from 1 to 13. The **module** *num* keyword and argument are supported on DFC-equipped modules and the standby supervisor engine only.

When you execute the **remote login module** *num* command, the prompt changes to Router-dfcx# or Switch-sp#, depending on the type of module to which you are connecting.

When you execute the **remote login standby-rp** command, the prompt changes to Router-sdby#.

When you execute the **remote login switch** command, the prompt changes to Switch-sp#.

The **remote login module** *num* command is identical to the **attach** command.

There are two ways to end the session:

- You can enter the **exit** command as follows:

```
Switch-sp# exit
```

```
[Connection to Switch closed by foreign host]
Router#
```

- You can press **Ctrl-C** three times as follows:

```
Switch-sp# ^C
Switch-sp# ^C
Switch-sp# ^C
Terminate remote login session? [confirm] y
[Connection to Switch closed by local host]
Router#
```

Examples

This example shows how to perform a remote login to a specific module:

```
Router# remote login module 1
Trying Switch ...
Entering CONSOLE for Switch
Type "^C^C^C" to end this session
Switch-sp#
```

This example shows how to perform a remote login to the Cisco 7600 series router processor:

```
Router# remote login switch
Trying Switch ...
Entering CONSOLE for Switch
Type "^C^C^C" to end this session
Switch-sp#
```

This example shows how to perform a remote login to the standby route processor:

```
Router# remote login standby-rp
Trying Switch ...
Entering CONSOLE for Switch
Type "^C^C^C" to end this session
Router-sdby#
```

Related Commands

Command	Description
attach	Connects to a specific module from a remote location.

reset (alarm-interface)

To reset the CPU in the alarm interface controller (AIC), use the **reset**command in alarm-interface mode.

reset

Syntax Description

This command has no arguments or keywords.

Command Default

No default behavior or values

Command Modes

Alarm-interface

Command History

Release	Modification
12.2(2)XG	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.

Usage Guidelines

A change in the AIC IP configuration might not take effect until the next time the card is started. Use the **reset** command to restart the card. This command does not have a **no** form.

Examples

The following example shows a message that might be returned after the **reset** command is entered:

```
Router(alarm-aic)# reset
Selected card in slot 1 restarted
```

Related Commands

Command	Description
alarm-interface	Enters alarm-interface mode and configures the AIC.

retry

To define the amount of time that must elapse before a connection is attempted to a failed server, use the **retry** command in interface configuration mode. To change the connection-reassignment threshold and client threshold to the default settings, use the **no** form of this command.

retry *retry-value*
no retry

Syntax Description

retry-value	Amount of time, in seconds, that must elapse after the detection of a server failure before a new connection is attempted to the server; valid values are from 1 to 3600.

Command Default

retry-value is **60**

Command Modes

real server configuration submode

Command History

Release	Modification
12.2(14)SX	Support for this command was introduced on the Supervisor Engine 720.
12.2(17d)SXB	Support for this command on the Supervisor Engine 2 was extended to Release 12.2(17d)SXB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Examples

This example shows how to specify a retry timer of 30 seconds:

```
Router(config)# ip slb serverfarm serverfarm-name
Router(config-slb-sfarm)# real 10.1.1.1
Cisco-7600(config-slb-real)# retry 30
```

This example shows how to revert to the default value:

```
Cisco-7600(config-slb-real)# no
 retry
Router(config-if)#
```

Related Commands

Command	Description
faildetect numconns	Specifies the conditions that indicate a server failure.
inservice (real server)	Enables the real server for use by the IOS SLB feature.
maxconns	Limits the number of active connections to the real server.

ring-speed

To set the ring speed for the CSC-1R and CSC-2R Token Ring interfaces, use the **ring-speed** command in interface configuration mode.

ring-speed commandring-speed *speed*

Syntax Description

speed	Integer that specifies the ring speed, either 4 for 4-Mbps operation or 16 for 16-Mbps operation . The default is 16.

Command Default

16-Mbps operation

Caution Configuring a ring speed that is wrong or incompatible with the connected Token Ring causes the ring to beacon, which makes the ring nonoperational.

Command Modes

Interface configuration

Command History

Release	Modification
10.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

This command does not have a **no** form.

Examples

The following example shows how to sets the ring speed to 4 Mbps on a Token Ring interfaces:

```
Router(config)# interface tokenring 0
Router(config-if)# ring-speed 4
```

rj45-auto-detect-polarity

To enable or disable polarity detection for 10 Mbps full-duplex links, use the **rj45-auto-detect-polarity** command in interface configuration mode.

rj45-auto-detect-polarity {**enable** | **disable**}

Syntax Description

enable	Enables polarity detection on the RJ45 interface.
disable	Disables polarity detection on the RJ45 interface.

Command Default

Polarity detection is disabled for 10 Mbps, full duplex links.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
15.0(1)M3	This command was introduced.

Usage Guidelines

This command is available only for 10 Mbps, full-duplex links. The polarity detection feature helps to detect reversed polarity and provide correction; however, there is a risk of cyclic redundancy check (CRC) errors if polarity detection is enabled.

The polarity detection feature is disabled by default. Use the **rj45-auto-detect-polarityenable**to enable polarity detection.

It is recommended to leave polarity detection disabled.

Examples

The following example shows how to enable polarity detection on the RJ45 interface:

```
router(config-if)# rj45-auto-detect-polarity enable
```

Related Commands

Command	Description
media-type auto-failover	Assigns the RJ45 or the SFP port as the primary and secondary failover media.