

I through K

- id aa-group, on page 3
- id software group, on page 4
- id vsat, on page 5
- idle-pattern, on page 6
- ids-service-module monitoring, on page 7
- if-mgr delete, on page 8
- ignore (interface), on page 9
- ignore-dcd, on page 11
- ignore-error-duration, on page 12
- ignore-hw local-loopback, on page 13
- imc access-port, on page 14
- imc config file, on page 17
- imc dns, on page 18
- imc ip address default-gateway, on page 19
- imc ip address dhcp, on page 20
- imc ip dhcp, on page 21
- imc remote-manager, on page 22
- imc vlan, on page 23
- input, on page 24
- interface, on page 25
- interface analysis-module, on page 39
- interface content-engine, on page 40
- interface fastethernet, on page 41
- interface gigabitethernet, on page 42
- interface group-async, on page 43
- interface integrated-service-engine, on page 44
- interface ism, on page 45
- interface port-channel, on page 46
- interface pos, on page 47
- interface range, on page 48
- interface satellite, on page 52
- interface service-engine, on page 53
- interface sm, on page 54

- interface vg-anylan, on page 55
- interface vmi, on page 56
- interface wlan-controller, on page 58
- international bit, on page 59
- inter-packet gap 6502-mode, on page 60
- invert data, on page 61
- invert rxclock, on page 63
- invert txclock, on page 64
- ip dscp, on page 65
- ip pxf, on page 66
- ip rbscp ack-split, on page 67
- ip verify unicast source reachable-via, on page 69
- ipc buffers, on page 75
- ipc header-cache, on page 76
- ipc holdq threshold, on page 77
- ipc master, on page 78
- ipc zone default, on page 79
- iphc-profile, on page 80
- keepalive, on page 84

id aa-group

To configure the asynchronous acknowledgement group ID, use the **idaa-group**command in satellite initial configuration mode. To remove the ID configuration, use the **no** form of this command.

id aa-group *number*
no id aa-group

Syntax Description

aa-group	Asynchronous acknowledgement group ID.
number	ID number in the range from 256 to 511.

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 asynchronous acknowledgement group identification number:

```
Router(sat-init-config)# id aa-group 336
```

id software group

To configure the operational software group identification number, use the **idsoftwaregroup**command in satellite initial configuration mode. To remove the ID configuration, use the **no** form of this command.

id software group *number*
no id software group

Syntax Description

number	ID number in the range from 512 to 767.

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 operational software group identification number:

```
Router(sat-init-config)# id software group 598
```

id vsat

To configure the component physical address (CPA), use the **idvsat**command in satellite initial configuration mode. To remove the CPA configuration, use the **no** form of this command.

id vsat *number*
no id vsat *number*

Syntax Description

number	CPA number in the range from 1280 to 32766.

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(22)T	The CPA number range was increased to 32766.

Usage Guidelines

The CPA uniquely identifies the VSAT endpoint in the satellite network.



Note 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 CPA number:

```
Router(sat-init-config)# id vsat 1284
```

idle-pattern

To define the idle pattern that a circuit emulation (CEM) channel transmits when the channel experiences an underrun condition or to replace any missing packets, use the **idle-pattern**command in CEM configuration mode. To stop sending idle pattern data, use the **no** form of this command.

idle-pattern {*pattern* | *length pattern1* [*pattern2*]}
no idle-pattern

Syntax Description

pattern	An 8-bit hexadecimal number. T1 and E1 channels require only this argument.
length	Length, in bits, of the pattern. Serial cards require that you enter a value for *length* .
pattern1	Specifies (in hex notation) up to 32 bits of the least significant bits of the idle data pattern. Default is 0xFF.
pattern2	(Optional) Specifies (in hex notation) the most significant bits of the idle data pattern. If the *length* argument is 32 bits or less, this argument is not permitted.

Command Default

For T1 or E1 channels, the default idle pattern is 0xFF. For serial channels, the default idle pattern is 0xFF and 8 bits in length.

Command Modes

CEM configuration

Command History

Release	Modification
12.3(7)T	This command was introduced.
XE 3.18SP	This command is integrated in Cisco NCS 4200 Series.

Usage Guidelines

Idle pattern data is always sent in multiples of one entire packet payload. If a single packet is missing from the arriving data stream it is replaced by an idle packet of the same payload size and composed of repetitions of the specified idle pattern. If the CEM channel outbound (egress) buffer experiences an underrun condition, identical idle packets are transmitted until the dejitter buffer is filled to at least half its total depth.

Examples

The following example shows how to configure a 32-bit idle pattern for a serial CEM channel.

```
Router(config-cem)# idle-pattern 32 0x12345678
```

Related Commands

Command	Description
cem	Enters circuit emulation configuration mode.
clear cem	Clears CEM channel statistics.
show cem	Displays CEM channel statistics.

ids-service-module monitoring

To enable Intrusion Detection System (IDS) monitoring on a specified interface, use the **ids-service-modulemonitoring** command in interface configuration mode. To perform IDS monitoring, the routing device must have a Cisco IDS network module installed. To disable IDS monitoring, use the **no** form of this command.

ids-service-module monitoring
no ids-service-module monitoring

Syntax Description

This command has no arguments or keywords.

Command Default

IDS monitoring is not enabled.

Command Modes

Interface configuration

Command History

Release	Modification
12.3(4)T	This command was introduced.

Usage Guidelines

Use the **ids-service-modulemonitoring** command to enable IDS monitoring on a specified interface or subinterface. Both inbound and outbound packets on the specified interface are forwarded for monitoring.

The Cisco IDS network module is also referred to as the NM-CIDS.

Examples

The following example shows how to configure Fast Ethernet interface 0/0 to copy network traffic to the Cisco IDS network module and enable IDS monitoring:

```
Router(config)# interface FastEthernet0/0
Router(config-if)# ids-service-module monitoring
```

Related Commands

Command	Description
service-module ids-sensor	Reboots, resets, enables console access to, shuts down, and monitors the status of the Cisco IDS network module.

if-mgr delete

To delete the unused interface identification numbers (ifIndex) from the system interface, use the **if-mgrdelete** command in privileged EXEC mode.

if-mgr delete {**ifindex-pool** *initial-ifindex number-of-ifindexes* | **interfaceType** *interface-name*}

Syntax Description

ifindex-pool	Specifies the ifIndex pool to delete.
initial-ifindex	Initial ifIndex value in the ifIndex pool. The range is from 1 to 3200.
number-of-ifindexes	The number of ifIndexes to be deleted. The range is from 1 to 3200.
interfaceType	Specifies the type of interface to which the ifIndex value is assigned.
interface-name	Name of the interface to which the ifIndex is assigned.

Command Default

The ifIndexes assigned for the specified system interface are deleted.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.2 SXH	This command was introduced.

Usage Guidelines

The ifIndex is a unique identification value associated with a physical or logical interface.

While specifying the ifIndex to be deleted, also provide the interface description (ifDescr) and the ifindex value assigned to that interface.

Examples

The following example shows how to delete the pool of unused ifIndexes:

```
Router# if-mgr delete ifindex-pool 2 5
```

Related Commands

Command	Description
show snmp mib ifmib ifindex	Displays all SNMP ifIndex identification numbers for all system interfaces.

ignore (interface)

To configure the serial interface to ignore the specified serial signals as the line up/down indicator, use the **ignore**command in interface configuration mode. To restore the default, use the **no** form of this command.

DCE Asynchronous Mode
ignore [**dtr** | **rts**]
no ignore [**dtr** | **rts**]

DCE Synchronous Mode
ignore [**dtr** | **local-loopback** | **rts**]
no ignore [**dtr** | **local-loopback** | **rts**]

DTE Asynchronous Mode
ignore [**cts** | **dsr**]
no ignore [**cts** | **dsr**]

DTE Synchronous Mode
ignore [**cts** | **dcd** | **dsr**]
no ignore [**cts** | **dcd** | **dsr**]

Syntax Description

dtr	Specifies that the DCE ignores the Data Terminal Ready (DTR) signal.
rts	Specifies that the DCE ignores the Request To Send (RTS) signal.
local-loopback	Specifies that the DCE ignores the local loopback signal.
cts	Specifies that the DTE ignores the Clear To Send (CTS) signal.
dsr	Specifies that the DTE ignores the Data Set Ready (DSR) signal.
dcd	Specifies that the DTE ignores the Data Carrier Detect (DCD) signal.

Command Default

The **no** form of this command is the default. The serial interface monitors the serial signal as the line up/down indicator.

Command Modes

Interface configuration

Command History

Release	Modification
12.2(15)ZJ	This command was introduced on the following platforms: Cisco 2610XM, Cisco 2611XM, Cisco 2620XM, Cisco 2621XM, Cisco 2650XM, Cisco 2651XM, Cisco 2691, Cisco 3631, Cisco 3660, Cisco 3725, and Cisco 3745 routers.
12.3(2)T	This command was integrated into Cisco IOS Release 12.3(2)T.

Usage Guidelines

Serial Interfaces in DTE Mode

When the serial interface is operating in DTE mode, it monitors the DCD signal as the line up/down indicator. By default, the attached DCE device sends the DCD signal. When the DTE interface detects the DCD signal, it changes the state of the interface to up.

SDLC Multidrop Environments

In some configurations, such as a Synchronous Data Link Control (SDLC) multidrop environment, the DCE device sends the DSR signal instead of the DCD signal, which prevents the interface from coming up. Use this command to tell the interface to monitor the DSR signal instead of the DCD signal as the line up/down indicator.

Examples

The following example shows how to configure serial interface 0 to ignore the DCD signal as the line up/down indicator:

```
Router(config)# interface serial 0
Router(config-if)# ignore dcd
```

Related Commands

Command	Description
debug serial lead-transition	Activates the leads status transition debug capability for all capable ports.
show interfaces serial	Displays information about a serial interface.

ignore-dcd

To configure the serial interface to monitor the Data Set Ready (DSR) signal instead of the Data Carrier Detect (DCD) signal as the line up/down indicator, use the **ignore-dcd** command in interface configuration mode. To restore the default, use the **no** form of this command.

ignore-dcd
no ignore-dcd

Syntax Description

This command has no arguments or keywords.

Command Default

The serial interface, operating in DTE mode, monitors the DCD signal as the line up/down indicator.

Command Modes

Interface configuration

Command History

Release	Modification
11.0	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 applies to Quad Serial NIM interfaces on the Cisco 4000 series routers and Hitachi-based serial interfaces on the Cisco 2500 and Cisco 3000 series routers.

Serial Interfaces in DTE Mode

When the serial interface is operating in DTE mode, it monitors the DCD signal as the line up/down indicator. By default, the attached DCE device sends the DCD signal. When the DTE interface detects the DCD signal, it changes the state of the interface to up.

SDLC Multidrop Environments

In some configurations, such as an Synchronous Data Link Control (SDLC) multidrop environment, the DCE device sends the DSR signal instead of the DCD signal, which prevents the interface from coming up. Use this command to tell the interface to monitor the DSR signal instead of the DCD signal as the line up/down indicator.

Examples

The following example shows how to configure serial interface 0 to monitor the DSR signal as the line up/down indicator:

```
Router(config)# interface serial 0
Router(config-if)# ignore-dcd
```

ignore-error-duration

To ignore initial train-up errors when the DSL controller is connected to DSLAMs with chipsets other than Globespan, use the**ignore-error-duration** command in controller configuration mode. To set the error duration to the default of 0 seconds, use the **no** form of the command.

ignore-error-duration *seconds*

Syntax Description

seconds	Sets the time in seconds for which errors will be ignored during training of the line. Range is from 15 to 30 seconds.

Command Default

0 seconds

Command Modes

Controller configuration

Command History

Release	Modification
12.3(4)XD	This command was introduced on Cisco 2600 series and Cisco 3700 series routers.
12.3(4)XG	This command was integrated into the Cisco IOS Release 12.3(4)XG on the Cisco 1700 series routers.
12.3(7)T	This command was implemented on Cisco 2600 series, Cisco 3631, and Cisco 3700 series routers.
12.3(11)T	This command was implemented on Cisco 2800 and Cisco 3800 series routers.
12.3(14)T	This command was implemented on Cisco 1800 series routers.

Usage Guidelines

This command is used to ignore initial train-up errors when connected to DSLAMs with chipsets other than Globespan. Use the time period of 15 to 30 seconds to allow the line to train without being affected by errors that result because of the line training.

Examples

The following example sets the time during which errors will be ignored to 15 seconds:

```
Router(config)# controller dsl
4/0
Router(config-controller)# ignore-error-duration
15
```

Related Commands

Command	Description
controller dsl	Configures the DSL controller.

ignore-hw local-loopback

To disable the monitoring of the (local-loopback) LL pin when in DCE mode, use the **ingnore-hwlocal-loopback** command in interface configuration mode. To enable the monitoring of the LL pin, use the **no** form of this command.

ignore-hw local-loopback
no ignore-hw local-loopback

Syntax Description

This command has no arguments or keywords.

Command Default

Enabled

Command Modes

Interface configuration

Command History

Release	Modification
11.3	This command was introduced.
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 this command if your system is experiencing spurious modem interrupts that momentarily cause the interface to enter loopback mode. The end result of this behavior is the loss of Synchronous Data Link Control (SDLC) Logical Link Control (SDLLC) sessions.



Note This command works only with the low-speed serial interfaces.

Examples

The following example shows how to disable the monitoring of the LL pin when in DCE mode:

```
Router(config)# interface serial 2
Router(config-if)# ignore-hw local-loopback
```

imc access-port

To configure Cisco Integrated Management Controller (CIMC) access through the server module's dedicated, management, or host ports, use the **imc access-port** command in interface configuration mode or UCSE configuration mode.

Cisco UCS E-Series Server Installed in Cisco 2900 and 3900 ISR G2 and the Cisco ISR 4451-X
imc access-port {**dedicated** | **shared-lom** [**GE1** | **GE2** | **GE3** | **console** | **failover** [*option*]]}
no imc access-port {**dedicated** | **shared-lom** [**GE1** | **GE2** | **GE3** | **console** | **failover** [*option*]]}

Cisco UCS E-Series Server Installed in the Cisco ISR 4451-X—Applicable Only with Cisco IOS XE Release 3.9S
imc access-port {**MGMT** | [**GE0** | **GE1** | **GE2** | **GE3**[*failover-option*]]}
no imc access-port {**MGMT** | [**GE0** | **GE1** | **GE2** | **GE3**[*failover-option*]]}

Syntax Description

Table 1: Cisco UCS E-Series Server Installed in Cisco 2900 and 3900 ISR G2 and the Cisco ISR 4451-X

dedicated	Configures CIMC access using the IMC dedicated port.
shared-lom	Configures CIMC access using one of the following host ports: • **GE1** • **GE2** • **GE3** • **console** • **failover** **Note** If you enter **failover**, you must also enter one additional parameter: • **GE1 GE1** [**GE2**] | [**GE3**] [**GE2 GE3**] • **GE2 GE2 GE3**

Table 2: Cisco UCS E-Series Server Installed in the Cisco ISR 4451-X—Applicable Only with Cisco IOS XE Release 3.9S

MGMT	Configures CIMC access using the Cisco UCS E-Series Server's management port.

GE0, **GE1**, **GE2**, **GE3**	(Optional) Configures CIMC access using one of the following NIC interfaces: • **GE0**—Cisco UCS E-Series Server's internal NIC interface connecting to the router's UCSE *slot*/**0/0** interface. • **GE1**—Cisco UCS E-Series Server's internal NIC interface connecting to the router's UCSE *slot*/**0/1** interface. • **GE2**—Cisco UCS E-Series Server's external NIC interface. • **GE3**—Cisco UCS E-Series Server's external NIC interface. Applicable to double-wide Cisco UCS E-Series Servers. • *failover-option*—To configure failover, enter one additional parameter: • **GE2 backplane**—Applicable to single-wide and double-wide Cisco UCS E-Series Servers. • **GE3 backplane**—Applicable to double-wide Cisco UCS E-Series Servers. • **GE2 GE3**—Applicable to double-wide Cisco UCS E-Series Servers. • **GE3 GE2**—Applicable to double-wide Cisco UCS E-Series Servers. • **GE2 GE3 backplane**—Applicable to double-wide Cisco UCS E-Series Servers. • **GE3 GE2 backplane**—Applicable to double-wide Cisco UCS E-Series Servers.

Command Modes

Interface configuration (config-if) for a Cisco UCS E-Series Server installed in Cisco 2900 and 3900 ISR G2.

UCSE configuration (config-ucse) for a Cisco UCS E-Series Server installed in the Cisco ISR 4451-X.

Command History

Release	Modification
Cisco IOS Release 15.2(4)M	This command was introduced on the Cisco UCS E-Series Servers installed in Cisco 2900 and 3900 Series Integrated Services Routers (ISR G2).
Cisco IOS XE Release 3.9S	This command was implemented on Cisco UCS E-Series Servers installed in the Cisco 4451-X Integrated Services Router (Cisco ISR 4451-X).
Cisco IOS XE Release 3.10S	This command was modified so that all platforms—Cisco 2900 and 3900 ISR G2 and the Cisco ISR 4451-X—use the same command.

Usage Guidelines

If the Cisco UCS E-Series Server is installed in Cisco 2900 and 3900 ISR G2, use the **imc access-port** command in interface configuration mode:

```
Router(config)# interface ucse 2/0
Router(config-if)#
```

If the Cisco UCS E-Series Server is installed in Cisco ISR 4451-X, use the **imc access port** command in UCSE configuration mode:

```
Router(config)# ucse subslot 1/0
Router(config-ucse)#
```

Examples

The following example shows how to configure CIMC access using the dedicated port:

```
Router# configure terminal
Router(config)# interface ucse 2/0
Router(config-if)# imc ip address 10.0.0.2 255.0.0.0 default-gateway 10.0.0.1
Router(config-if)# imc access-port dedicated
Router(config-if)# no shut
Router(config-if)# end
```

Cisco UCS E-Series Server Installed in the Cisco ISR 4451-X—Applicable Only with Cisco IOS XE Release 3.9S

The following example shows how to configure CIMC access using the MGMT port:

```
Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# ucse subslot 1/0
Router(config-ucse)# imc access-port mgmt
Router(config-ucse)#
 IMC ACK: Access ports received: MGMT

 IMC ACK: UCSE access port operation successful.
```

imc config file

To store the name of a CIMC configuration file in the running configuration, use the **imc config file** command from interface configuration mode .

imc config file *file_name*
no imc config file *file_name*

Syntax Description

file_name	The name of the CIMC configuration file that you want to store.

Command Modes

Interface configuration mode.

Command History

Release	Modification
15.2(4)M	This command was introduced.

Usage Guidelines

Use this command from interface configuration mode:

```
Router(config)# interface ucse slot/port
```

Examples

The following example shows how to store a configuration CIMC file to the running configuration. Note that there is no output after you issue the command:

```
Router(config)# interface ucse 2/0
Router(config-if)# imc config file flash0:my-imc-config
```

imc dns

To configure a domain name system (DNS) server for CIMC, use the **imc dns** command from interface configuration mode.

imc dns
no imc dns

Syntax Description

This command has no arguments.

Command Modes

Interface configuration mode.

Command History

Release	Modification
15.2(4)M	This command was introduced.

Usage Guidelines

Use this command from interface configuration mode:

```
Router(config)# interface ucse slot/port
```

Examples

The following example shows how to configure the DNS server for CIMC:

```
Router(config)# interface ucse 2/0
Router(config-if)# imc dns
```

imc ip address default-gateway

To configure a static IP address for CIMC and the IP address of the default gateway router that CIMC must use, use the **imc ip address default-gateway** command in interface configuration mode. To remove the static IP address, use the **no** form of this command.

imc ip address *ip-address subnet-mask* **default-gateway** *gateway-address*
no imc ip address *ip-address subnet-mask* **default-gateway** *gateway-address*

Syntax Description

ip-address	IP address of CIMC.
subnet-mask	Subnet mask to append to the IP address; must be in the same subnet as the host router.
gateway-address	IP address of the default gateway router.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
15.2(4)M	This command was introduced.

Usage Guidelines

If you do not enable DHCP, you must specify a static IP address and subnet mask.

Examples

The following example shows how to configure a static IP address for CIMC:

```
Router(config)# interface ucse 2/0
Router(config-if)# imc ip address 10.0.0.2 255.0.0.0 default-gateway 10.0.0.1
```

imc ip address dhcp

To configure a DHCP IP address for CIMC, use the **imc ip address dhcp** command in interface configuration mode. To remove the DHCP IP address, use the **no** form of the this command.

imc ip address dhcp
no imc ip address dhcp

Syntax Description

This command has no arguments or keywords.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
15.2(4)M	This command was introduced.

Examples

The following example shows how to configure a DHCP IP address for CIMC:

```
Router(config)# interface ucse 2/0
Router(config-if)# imc ip address dhcp
```

imc ip dhcp

To configure a DHCP IP address for the Cisco Integrated Management Controller (CIMC), use the **imc ip dhcp** command in UCSE configuration mode. To remove the DHCP IP address, use the **no** form of this command.

imc ip dhcp
no imc ip dhcp

Syntax Description

This command has no arguments or keywords.

Command Modes

UCSE configuration (config-ucse)

Command History

Release	Modification
Cisco IOS XE Release 3.9S	This command was introduced on the Cisco UCS E-Series Servers installed in the Cisco 4400 Series Integrated Services Router (ISR).

Examples

The following example shows how to configure a dynamic IP address for CIMC:

```
Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# ucse subslot 1/0
Router(config-ucse)# imc ip dhcp
Router(config-ucse)#
 IMC ACK: DHCP enable received for IMC.

 IMC ACK: UCSE setting DHCP enable for IMC successful.
```

imc remote-manager

To configure the IP address of the remote manager, use the **imc remote-manager** command from interface configuration mode .

imc remote-manager *ip_address*
no imc remote-manager

Syntax Description

ip_address	IP address of the remote manager.

Command Modes

Interface configuration mode.

Command History

Release	Modification
15.2(4)M	This command was introduced.

Usage Guidelines

Use this command from interface configuration mode:

```
Router(config)# interface ucse slot/port
```

Examples

The following example shows how to configure the IP address of the remote manager:

```
Router(config)# interface ucse 2/0
Router(config-if)# imc remote-manager 10.0.0.0
```

imc vlan

To enter VLAN configuration mode for the specified VLAN number, use the **imc vlan** command in interface configuration mode. To remove the VLAN configuration, use the **no** form of this command.

imc vlan *vlan-number*
no imc vlan *vlan-number*

Syntax Description

vlan-number	IP address of the remote manager.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
15.2(4)M	This command was introduced.

Examples

The following example shows how to enter VLAN configuration mode in CIMC for a specified VLAN:

```
Router(config)# interface ucse 2/0
Router(config-if)# interface vlan 40
```

input

To enable Precision Time Protocol input clocking using a 1.544Mhz, 2.048Mhz, or 10Mhz timing interface or phase using the 1PPS or RS-422 interface, use the **input** command in global configuration mode. To disable PTP input, use the **no** form of this command.

input [**1pps**] *slot*/*bay*
no input [**1pps**] *slot*/*bay*

Syntax Description

1pps	Configures the device to receive 1 pulse per second (1PPS) time of day messages using the RS422 port or 1PPS port. You can select 1PPS with or without selecting a timing port.
slot	Slot of the 1PPS interface.
bay	Bay of the 1PPS interface.

Command Default

Precision Time Protocol input clocking 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.

Usage Guidelines

If you are using GPS to provide clock source to the device, configure this command in PTP master mode.

This command applies only to platforms that have a 1PPS port.

Examples

The following example shows how to configure PTP input clocking:

```
Device> enable
Device# configure terminal
Device(config)# ptp clock ordinary domain 0
Device(config-ptp-clk)# input 1pps 3/1
Device(config-ptp-clk)# clock-port masterport master
```

Related Commands

Command	Description
output	Enables output of time of day messages using the 1PPS interface.

interface

To configure an interface type and to enter interface configuration mode, use the **interface** command in the appropriate configuration mode.

Standard Syntax
interface *type number* [*name-tag*]

Module-Specific and Platform-Specific Syntax

Analysis Module Network Module
interface analysis-module *slot/unit*

Content Engine Network Module
interface content-engine *slot/unit*

Cisco 830 Series
interface *type* [*number*]

Cisco 2600 Series
interface *type slot/* {*port-adapter* | *port* **.** *subinterface-number*}

Cisco 2600 Series on Voice Interfaces
interface *type slot/voice-module-slot/voice-interface-slot*

Cisco 3600 Series
interface *type slot/* {*port* | *port* **.** *subinterface-number*}

Cisco 3600 Series on Voice Interfaces
interface *type slot/voice-module-slot/voice-interface-slot*

Cisco 4400 Series Integrated Services Router (ISR)
interface *type number*

Cisco 7100 Series
interface *type slot/* {*port-adapter* | *port* **.** *subinterface-number*}

Cisco 7200 Series and Cisco 7500 Series with a Packet over SONET Interface Processor
interface *type slot/port*

Cisco 7200 VXR Router Used as a Router Shelf in a Cisco AS5800 Universal Access Server
interface *type router-shelf/slot/port*

Cisco 7500 Series with Channelized T1 or E1
interface serial *slot/port* **:** *channel-group*

Cisco 7500 Series with Ports on VIP Cards
interface *type slot/port-adapter/port*

Cisco 7600 Series
interface *type number*

Note: The number format varies depending on the network module or line card type and the router's chassis slot it is installed in. Refer to the appropriate hardware manual for numbering information

Cisco 7600 Series with Ports on Ethernet Service Cards
interface type *slot/bay/port* **access**

Note: The syntax may vary depending on the Ethernet service line card type. Refer to the appropriate hardware manual for numbering information. For example, for the ES20 line card the syntax takes the following format:

Subinterface Syntax Forms in Global Configuration Mode

Cisco 7200 Series
interface *type slot/port* **.** *subinterface-number* [**multipoint** | **point-to-point**]

Cisco 7500 Series
interface *type slot/port-adapter* **.** *subinterface-number* [**multipoint** | **point-to-point**]

Cisco 7500 Series with Ports on VIP Cards
interface *type slot/port-adapter/port* **.** *subinterface-number* [**multipoint** | **point-to-point**]

Cisco ASR 901 Series Aggregation Services Routers
no interface *type number*

Shared Port Adapters
interface *type slot/subslot/port* [**.** *subinterface-number*]

Syntax Description

type	Type of interface to be configured. See the table below.
number	Port, connector, or interface card number. On Cisco 830 series routers, the *number*argumentspecifies the ethernet interface number. On Cisco 4700 series routers, the number argument specifies the network interface module (NIM) or network processor module (NPM) number. The numbers are assigned at the factory at the time of installation or when added to a system; they can be displayed with the **showinterfaces** command. For Cisco ASR 901 Series Aggregation Services Routers, the range is from 1 to 8.
name-tag	(Optional) Specifies the logic name to identify the server configuration so that multiple server configurations can be entered. This optional argument is for use with the Redundant Link Manager (RLM) feature.
slot	Chassis slot number. Refer to the appropriate hardware manual for slot information. For SIPs, refer to the platform-specific SPA hardware installation guide or the corresponding "Identifying Slots and Subslots for SIPs and SPAs" topic in the platform-specific SPA software configuration guide.

/ *voice-module-slot*	Voice module slot number. The slash(/)is required. Refer to the “Cisco 3700 Series Routers Voice Interface Numbering” section of the “Understanding Interface Numbering and Cisco IOS Basics” chapter in the platform-specific SPA software configuration guide.
/ *voice-interface-slot*	Voice interface slot number. The slash(/)is required. Refer to the “Cisco 3700 Series Routers Voice Interface Numbering” section of the “Understanding Interface Numbering and Cisco IOS Basics” chapter in the platform-specific SPA software configuration guide.
/ *subslot*	Secondary slot number on a SIP where a SPA is installed. The slash (/) is required. Refer to the platform-specific SPA hardware installation guide and the corresponding "Specifying the Interface Address on a SPA" topic in the platform-specific SPA software configuration guide for subslot information.
/ *unit*	Number of the daughter card on the network module. For analysis module and content engine (CE) network modules, always use 0. Theslash(/)is required.
/bay	Card interface bay number in a slot. Theslash(/)is required. Refer to the appropriate hardware manual for bay information.
/ *port*	Port or interface number. Theslash(/)is required. Refer to the appropriate hardware manual for port information. For SPAs, refer to the corresponding “Specifying the Interface Address on a SPA” topics in the platform-specific SPA software configuration guide.
router-shelf	Router shelf number in a Cisco AS5800 universal access server. Refer to the appropriate hardware manual for router shelf information.
: *channel-group*	Channel group number. Cisco 7500 series routers specify the channel group number in the range of 0 to 4 defined with the **channel-group** controller configuration command.
/ *port-adapter*	Port adapter number. Refer to the appropriate hardware manual for information about port adapter compatibility. Theslash(/) is required.
. *subinterface-number*	Subinterface number in the range 1 to 4294967293. The number that precedes the period (.) must match the number to which this subinterface belongs.
access	Creates an access interface for an IP subscriber. The access interface is configured as a subinterface of the physical interface that the IP subscriber is connected to.
multipoint | **point-to-point**	(Optional) Specifies a multipoint or point-to-point subinterface. There is no default .

Command Default

No interface types are configured.

Command Modes

Global configuration (config)

RITE configuration (config-rite)

Note To use this command with the RLM feature, the networking device must be in interface configuration mode.

Command History

Release	Modification
10.0	This command was introduced for the Cisco 7000 series routers.
11.0	This command was implemented on the Cisco 4000 series routers.
12.0(3)T	The optional *name-tag*argument was added for the RLM feature.
12.2(13)T	The **content-engine** keyword was added.
12.2(15)T	The **lex** keyword was removed because the LAN Extension feature is no longer available in Cisco IOS software.
12.2(20)S2	This command was implemented for SPAs on the Cisco 7304 router.
12.3(4)T	The **serviceengine** keyword was added. Support was added for the **interface** command to be used in RITE configuration mode to support IP trfaffic export profiles.
12.3(7)T	The **analysis-module** keyword was added.
12.2(22)S	Support for RITE configuration mode and IP traffic export profiles was added.
12.3(14)T	The **satellite** keyword was added to support satellite interface configuration on network modules.
12.2(18)SXE	This command was implemented for SPAs on the Cisco 7600 series routers and Catalyst 6500 series switches.
12.0(31)S	This command was implemented for SPAs on the Cisco 12000 series routers.
12.2(18)SXF	The **tengigabitethernet** keyword was added for support of the10 Gigabit Ethernet interface type.
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.
Cisco IOS XE 2.1	This command was implemented on Cisco ASR 1000 series routers.
15.1(2)SNG	This command was implemented on Cisco ASR 901 Series Aggregation Services Routers.
Cisco IOS XE Release 3.9S	This command was implemented on Cisco 4400 Series ISR.
15.2(02)SA	This command was implemented on Cisco ME 2600X Series Ethernet Access Switches.
15.1(2)SNG	This command was implemented on Cisco ASR 901 Series Aggregation Services Routers.

Usage Guidelines

This command does not have a **no** form except for Cisco ASR 901 Series Aggregation Services Routers.

The table below displays the keywords that represent the types of interfaces that can be configured with the **interface** command. Replace the *type* argument with the appropriate keyword from the table.

Table 3: Interface Type Keywords

Keyword	Interface Type
analysis-module	Analysis module interface. The analysis module interface is a Fast Ethernet interface on the router that connects to the internal interface on the Network Analysis Module (NAM). This interface cannot be configured for subinterfaces or for speed, duplex mode, and similar parameters. See the command-line interface (CLI) help for a list of valid parameters.
async	Port line used as an asynchronous interface.
atm	ATM interface.
bri	ISDN BRI. This interface configuration is propagated to each of the B channels. B channels cannot be individually configured. The interface must be configured with dial-on-demand commands in order for calls to be placed on that interface.
content-engine	Content engine (CE) network module interface. The CE network module interface cannot be configured for subinterfaces or for speed, duplex mode, and similar parameters. See the command-line interface (CLI) help for a list of valid parameters. **Note** The **content-engine** keyword was formerly documented as the **interfacecontent-engine** command.
dialer	Dialer interface.
ethernet	Ethernet IEEE 802.3 interface.
fastethernet	100-Mbps Ethernet interface. In RITE configuration mode, specifies the outgoing (monitored) interface for exported IP traffic. **Note** The **fastethernet** keyword was formerly documented as the **interfacefastethernet** command.
fddi	FDDI interface.
gigabitethernet	1000-Mbps Ethernet interface. **Note** The **gigabitethernet** keyword was formerly documented as the **interfacegigabitethernet** command.
group-async	Master asynchronous interface. **Note** The **group-async** keyword was formerly documented as the **interfacegroup-async** command.

Keyword	Interface Type
hssi	High-Speed Serial Interface (HSSI).
loopback	Software-only loopback interface that emulates an interface that is always up. It is a virtual interface supported on all platforms. The *number* argument is the number of the loopback interface that you want to create or configure. There is no limit on the number of loopback interfaces that you can create.
null	Null interface.
port-channel	Port channel interface. **Note** The **port-channel** keyword was formerly documented as the **interfaceport-channel** command.
pos	Packet OC-3 interface on the Packet-over-SONET (POS) interface processor. **Note** The **pos** keyword was formerly documented as the **interfacepos** command.
Satellite	Satellite network module. Enters satellite configuration mode.
sdcc	Section data communications channel interface.
serial	Serial interface.
service-engine	Network module (NM) or an Advanced Integration Module (AIM), this command may be used for NMs and AIMs only. If your system does not have this hardware, you will be unable to enter this command. The no form of this command (no interface service-engine) is not available. The exit command can be used to exit interface configuration mode.
switch	Switch interface.
tengigabitethernet	10-Gigabit Ethernet interface.
tokenring	Token Ring interface.
tunnel	Tunnel interface; a virtual interface. The *number* argument is the number of the tunnel interface that you want to create or configure. There is no limit on the number of tunnel interfaces that you can create.
vg-anylan	100VG-AnyLAN port adapter. **Note** The **vg-anylan** keyword was formerly documented as the **interfacevg-anylan** command.

Creating an IP Traffic Export Profile

Ip traffic export is intended only for software switching platforms; distributed architectures are not supported.

After you configure an IP traffic export profile using the **iptraffic-exportprofile**global configuration command, you must also include the **interface**command after the **iptraffic-exportprofile**command; otherwise, the profile will be unable to export the captured IP packets. If you do not use the **interface** command, you will receive a warning that indicates that the profile is incomplete.

Subinterfaces

Subinterfaces can be configured to support partially meshed Frame Relay networks. Refer to the "Configuring Serial Interfaces" chapter in the *CiscoIOSInterfaceandHardwareComponentConfigurationGuide*.

Using the analysis-module Keyword

The analysis module interface is used to access the NAM console for the initial configuration. After the NAM IP parameters are configured, the analysis module interface is typically used only during NAM software upgrades and while troubleshooting if the NAM Traffic Analyzer is inaccessible.

Visible only to the Cisco IOS software on the router, the analysis module interface is an internal Fast Ethernet interface on the router that connects to the internal NAM interface. The analysis module interface is connected to the router's Peripheral Component Interconnect (PCI) backplane, and all configuration and management of the analysis module interface must be performed from the Cisco IOS CLI.

Using the group-async Keyword

Using the **group-async** keyword, you create a single asynchronous interface with which other interfaces are associated as members using the **group-range**command. This one-to-many configuration allows you to configure all associated member interfaces by entering one command on the group master interface, rather than entering this command on each individual interface. You can create multiple group masters on a device; however, each member interface can be associated only with one group.

Using the port-channel Keyword

The Fast EtherChannel feature allows multiple Fast Ethernet point-to-point links to be bundled into one logical link to provide bidirectional bandwidth of up to 800 Mbps. You can configure the port-channel interface as you would any Fast Ethernet interface.

After you create a port-channel interface, you assign upto four Fast Ethernet interfaces to it. For information on how to assign a Fast Ethernet interface to a port-channel interface, refer to the **channel-group** command in the interface configuration mode.



Caution The port-channel interface is the routed interface. Do not enable Layer 3 addresses on the physical Fast Ethernet interfaces. Do not assign bridge groups on the physical Fast Ethernet interfaces because doing so creates loops. Also, you must disable spanning tree.



Caution With Release 11.1(20)CC, the Fast EtherChannel supports Cisco Express Forwarding (CEF) and distributed Cisco Express Forwarding (dCEF). We recommend that you clear all explicit**iproute-cachedistributed** commands from the Fast Ethernet interfaces before enabling dCEF on the port-channel interface. Clearing the route cache gives the port-channel interface proper control of its physical Fast Ethernet links. When you enable CEF/dCEF globally, all interfaces that support CEF/dCEF are enabled. When CEF/dCEF is enabled on the port-channel interface, it is automatically enabled on each of the Fast Ethernet interfaces in the channel group. However, if you have previously disabled CEF/dCEF on the Fast Ethernet interface, CEF/dCEF is not automatically enabled. In this case, you must enable CEF/dCEF on the Fast Ethernet interface.

As you work with the **port-channel**keyword, consider the following points:

- Currently, if you want to use the Cisco Discovery Protocol (CDP), you must configure it only on the port-channel interface and not on the physical Fast Ethernet interface.
- If you do not assign a static MAC address on the port-channel interface, the Cisco IOS software automatically assigns a MAC address. If you assign a static MAC address and then later remove it, Cisco IOS software automatically assigns a MAC address.
- The **access** keyword creates an ethernet channel access interface for an IP subscriber and is specific to Cisco 7600 series routers only. For more information on access interface, see IP Subscriber Interfaces.

Using the vg-anylan Keyword

The 100VG-AnyLAN port adapter provides a single interface port that is compatible with and specified by IEEE 802.12. The 100VG-AnyLAN port adapter provides 100 Mbps over Category 3 or Category 5 cable with RJ-45 terminators and supports IEEE 802.3 Ethernet packets.

You configure the 100VG-AnyLAN port adapter as you would any Ethernet or Fast Ethernet interface. The 100VG-AnyLAN port adapter can be monitored with the IEEE 802.12 Interface MIB.

Cisco ASR 901 Series Aggregation Services Routers

The first EtherChannel interface configured becomes the bundled master for all EtherChannel interfaces in the group. That is, the MAC address of the first EtherChannel interface is the MAC address for all EtherChannel interfaces in the group. If the first EtherChannel interface is removed at any time, the second EtherChannel interface becomes the bundled master by default.

Repeat this configuration on every EtherChannel port to be bundled into a Fast Ether Channel (FEC) or Gigabit Ether Channel (GEC) group. This configuration must be present on all EtherChannel interfaces before the EtherChannel group can be configured.

Cisco 4400 Series Integrated Services Router (ISR)

The Gigabit Ethernet interface allows you to perform management tasks on the router and is often referred as the management interface port. You can use the Gigabit Ethernet interface to access the router via Telnet and SSH to perform management tasks on the router. The interface is most useful before a router has begun routing, or in troubleshooting scenarios when other forwarding interfaces are inactive. You can configure a Gigabit Ethernet interface on your router using the **interface GigabitEthernet0** command in Global configuration mode.

Analysis Module Interface with NAM Router: Example

The following example configures an analysis module interface when the NAM router is in router slot 1:

```
Router(config)# interface analysis-module 1/0
```

Asynchronous Group Master Interface: Example

The following example shows how to define asynchronous group master interface 0:

```
Router(config)# interface group-async 0
```

Content Engine Network Module Interface: Example

The following example configures an interface for a content engine network module in slot 1:

```
Router(config)# interface content-engine 1/0
```

Ethernet Interface on Cisco 830 Router: Example

The following example configures a new **ethernet2**interface on the LAN or on the WAN side of the Cisco 830 series router.

```
c837# configure terminal

Enter configuration commands, one per line.  End with CNTL/Z.
c837(config)# interface ethernet 2
```

Ethernet Port on Ethernet Interface Processor on Cisco 7500 Series Router: Example

The following example shows how to configure Ethernet port 4 on the Ethernet Interface Processor (EIP) in slot 2 on the Cisco 7500 series router:

```
Router(config)# interface ethernet 2/4
```

Exporting IP Traffic (RITE): Example

The following example shows how to configure the profile “corp1,” which will send captured IP traffic to host “00a.8aab.90a0” at the interface “FastEthernet 0/1.” This profile is also configured to export one in every 50 packets and to allow incoming traffic only from the access control list “ham_ACL.”

```
Router(config)# ip traffic-export profile corp1
Router(config-rite)# interface FastEthernet 0/1
Router(config-rite)# bidirectional
Router(config-rite)# mac-address 00a.8aab.90a0
Router(config-rite)# outgoing sample one-in-every 50
Router(config-rite)# incoming access-list ham_acl
Router(config-rite)# exit
Router(config)# interface FastEthernet 0/0
Router(config-if)# ip traffic-export apply corp1
```

Fast Ethernet Interface on Cisco 2600 Router: Example

The following example shows how to configure Fast Ethernet interface 0 on a Cisco 2600 series router:

```
Router(config)# interface fastethernet0/0
```

or

```
Router(config)# interface fastethernet0/0.1
```

Fast Ethernet Interface on Cisco 3600 Router: Example

The following example shows how to configure Fast Ethernet interface 0 on a Cisco 3600 series router:

```
Router(config)# interface fastethernet0/0
```

or

```
Router(config)# interface fastethernet0/0.1
```

Fast Ethernet Interface with ARPA Encapsulation on Cisco 4700 Router: Example

The following example shows how to configure Fast Ethernet interface 0 for standard ARPA encapsulation (the default setting) on a Cisco 4700 series router:

```
Router(config)# interface fastethernet 0
```

Fast Ethernet Interface on Cisco 7100 Router: Example

The following example shows how to configure Fast Ethernet interface 0 on a Cisco 7100 series router:

```
Router(config)# interface fastethernet0/0
```

or

```
Router(config)# interface fastethernet0/0.1
```

Fast Ethernet Interface on Cisco 12000 Router: Example

The following example shows how to configure Fast Ethernet interface 6 on a Cisco 12000 series router:

```
Router(config)# interface fastethernet6/0
```

or

```
Router(config)# interface fastethernet6/0.1
```

Gigabit Ethernet Interface: Example

The following example shows how to configure the Gigabit Ethernet interface for slot 0, port 0:

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

Gigabit Ethernet Interface on Cisco 4400 Series ISR: Example

The following example shows how to configure the Gigabit Ethernet Interface. The Gigabit Ethernet Interface or the management port is always GigabitEthernet0.

```
Router# config t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# interface gigabitethernet0
Router(config-if)#
```

Gigabit Ethernet Interface on Cisco uBR10012 Router: Example

The following example shows how to specify the second interface (1) on a Gigabit Ethernet SPA installed in the first subslot of a SIP (0) installed in chassis slot 3:

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

Loopback Interface: Example

The following example shows how to enable loopback mode and assign an IP network address and network mask to the interface. The loopback interface established here will always appear to be up.

```
Router(config)# interface loopback 0
Router(config-if)# ip address 10.108.1.1 255.255.255.0
```

Packet over SONET Interface: Example

The following example shows how to specify the single Packet OC-3 interface on port 0 of the POS OC-3 port adapter in slot 2:

```
Router(config)# interface pos 2/0
```

Partially Meshed Frame Relay Network: Example

The following example shows how to configure a partially meshed Frame Relay network. In this example, subinterface serial 0.1 is configured as a multipoint subinterface with two associated Frame Relay permanent virtual connections (PVCs), and subinterface serial 0.2 is configured as a point-to-point subinterface.

```
Router(config)# interface serial 0
Router(config-if)# encapsulation frame-relay
Router(config-if)# exit
Router(config)# interface serial 0/0.1 multipoint
Router(config-if)# ip address 10.108.10.1 255.255.255.0
Router(config-if)# frame-relay interface-dlci 42 broadcast
Router(config-if)# frame-relay interface-dlci 53 broadcast
Router(config-if)# exit
Router(config)# interface serial 0/0.2 point-to-point
```

```
Router(config-if)# ip address 10.108.11.1 255.255.255.0
Router(config-if)# frame-relay interface-dlci 59 broadcast
```

Port Channel Interface: Example

The following example shows how to create a port-channel interface with a channel group number of 1 and add two Fast Ethernet interfaces to port-channel 1:

```
Router(config)# interface port-channel 1
Router(config-if)# ip address 10.1.1.10 255.255.255.0
Router(config-if)# exit
Router(config)# interface fastethernet 1/0/0
Router(config-if)# channel-group 1
Router(config-if)# exit
Router(config)# interface fastethernet 4/0/0
Router(config-if)# channel-group 1
```

SDCC Interface on a POS Shared Port Adapter: Example

The following example configures the first interface (port 0) as a section data communications channel (SDCC) interface on a POS SPA, where the SPA is installed in the top subslot (0) of the MSC, and the MSC is installed in slot 4 of the Cisco 7304 router:

```
Router(config)# interface sdcc 4/3/0
Router(config-if)# ip address 10.1.9.2 255.255.255.0
Router(config-if)# logging event link-status
Router(config-if)# load-interval 30
Router(config-if)# no keepalive
Router(config-if)# no fair-queue
Router(config-if)# no cdp enable
```

Serial Interface with PPP Encapsulation: Example

The following example shows how to configure serial interface 0 with PPP encapsulation:

```
Router(config)# interface serial 0
Router(config-if)# encapsulation ppp
```

Shared Port Adapter Interface: Example

The following example configures the second interface (port 1) on a 4-Port 10/100 Fast Ethernet SPA for standard ARPA encapsulation (the default setting), where the SPA is installed in the bottom subslot (1) of the MSC, and the MSC is installed in slot 2 of the Cisco 7304 router:

```
Router(config)# interface fastethernet 2/1/1
```

T1 Serial Interface: Example

The following example shows how to configure circuit 0 of a T1 link for PPP encapsulation:

```
Router(config)# controller t1 4/1
Router(config-controller)# circuit 0 1
Router(config-controller)# exit
Router(config)# interface serial 4/1:0
Router(config-if)# ip address 10.108.13.1 255.255.255.0
Router(config-if)# encapsulation ppp
```

Token Ring Interface Processor: Example

The following example shows how to configure the Token Ring interface processor in slot 1 on port 0 of a Cisco 7500 series router:

```
Router(config)# interface tokenring 1/0
```

100VG-AnyLAN Interface: Example

The following example shows how to specify the 100VG-AnyLAN port adapter in the first port adapter in slot 1:

```
Router(config)# interface vg-anylan 1/0/0
```

Related Commands

Command	Description
channel-group	Defines the time slots that belong to each T1 or E1 circuit.
channel-group (Fast EtherChannel)	Assigns a Fast Ethernet interface to a Fast EtherChannel group.
clear interface	Resets the hardware logic on an interface.
controller	Configures an E1, J1, T1, or T3 controller and enters controller configuration mode.
group-range	Creates a list of asynchronous interfaces that are associated with a group interface on the same device.
ip traffic-export profile	Create or edit an IP traffic export profile.
mac-address	Sets the MAC layer address.
ppp	Starts an asynchronous connection using PPP.
show controllers content-engine	Displays controller information for CE network modules.
show interfaces	Displays information about interfaces.
show interfaces	Displays information about interfaces.
show interfaces content-engine	Displays basic interface configuration information for a CE network module.
shutdown (RLM)	Shuts down all of the links under the RLM group.

Command	Description
slip	Starts a serial connection to a remote host using SLIP.

interface analysis-module

To configure the Analysis-Module interface on the router that connects to an installed Network Analysis Module (NM-NAM), use the **interfaceanalysis-module** command in global configuration mode. This command does not have a not form.

interface analysis-module *slot*/*unit*

Syntax Description

slot	Number of the router chassis slot for the network module.
/ *unit*	Number of the daughter card on the network module. For NM-NAM, always use 0. The slash (/) between the slot and unit arguments is required.

Command Default

The interface is not configured.

Command Modes

Global configuration

Command History

Release	Modification
12.3(4)XD	This command was introduced on the following platforms: Cisco 2600XM series, Cisco 2691, Cisco 3660, Cisco 3725, and Cisco 3745.
12.3(7)T	This command was integrated into Cisco IOS Release 12.3(7)T.
12.3(8)T4	This command was implemented on the following platforms: Cisco 2811, Cisco 2821, and the Cisco 2851 series.
12.3(11)T	This command was made available on the Cisco 3800 series.

Usage Guidelines

The Analysis-Module interface is a Fast Ethernet interface on the router that connects to the internal interface on the Network Analysis Module (NM-NAM).

This type of interface cannot be configured for subinterfaces or for speed, duplex mode, and similar parameters. See the command-line interface (CLI) help for a list of valid parameters.

The **interfaceanalysis-module**command enters Analysis-Module interface configuration mode.

Examples

The following example shows how to configure the Analysis-Module interface when the NM-NAM is in router slot 1:

```
Router(config)# interface analysis-module 1/0
```

Related Commands

Command	Description
ip unnumbered	Enables IP processing on an interface without assigning an explicit IP address to the interface.
show interfaces analysis-module	Displays status, traffic data, and configuration information about the Analysis-Module interface.

interface content-engine

The **interfacecontent-engine**command is now documented as the **content-engine**keyword of the **interface** command. For more information, see the **interface**command.

interface fastethernet

The **interfacefastethernet**command is now documented as the **fastethernet**keyword of the **interface** command. For more information, see the **interface** command.

interface gigabitethernet

The **interfacegigabitethernet**command is now documented as the **gigabitethernet**keyword of the **interface** command. For more information, see the interface command.

interface group-async

The **interfacegroup-async**command is now documented as the **group-async**keyword of the **interface** command. For more information, see the **interface** command.

interface integrated-service-engine

To configure the Cisco wireless LAN controller network module (WLCM) interface with dot1q encapsulation on the router, use the **interfaceintegrated-service-engine** command.

interface integrated-service-engine slot/unit

Syntax Description

slot/unit	Specifies the router slot and unit numbers for the WLCM.

Command Default

None

Command Modes

Global configuration

Command History

Release	Modification
12.4(15)T	This command was introduced.

Examples

The following example shows how to create dot1Q virtual LAN (VLAN) subinterfaces under the **interfaceintegrated-service-engine** command:

```
Router(config)# interface integrated-service-engine
 1/0
Router(config-if)# exit
Router(config)# interface integrated-service-engine
 1/0.10
Router(config-subif)# encapsulation dot1q
 10

If the interface doesn't support baby giant frames
maximum mtu of the interface has to be reduced by 4
bytes on both sides of the connection to properly
transmit or receive large packets. Please refer to
documentation on configuring IEEE 802.1Q vLANs.

Router(config-subif)# end
```

Related Commands

show interfaces integrated-service-engine

interface ism

To configure an interface on the router that connects to an internal service module (ISM), use the **interfaceism** command in global configuration mode. This command does not have a no form.

interface ism *slot*/*port*

Syntax Description

slot	Router slot in which the service module is installed. For internal service modules, always use 0.
/ *port*	Port number of the module interface. Range: 0 or 1. The slash mark (/) is required.

Command Default

The interface is not configured.

Command Modes

Global configuration (config)

Command History

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

Usage Guidelines

This command enters interface configuration mode to configure the interface between the router and the ISM or between the ISM and Multi-Gigabit Fabric (MGF).

Examples

The following example shows how to enter interface configuration mode for the ISM:

```
Router(config)# interface ism 0/0
```

Related Commands

Command	Description
ip unnumbered	Enables IP processing on an interface without assigning an explicit IP address to the interface.
service-module ip address	Specifies the IP address of the module side of the interface.
show interfaces ism	Displays status, traffic data, and configuration information about the ISM interface.

interface port-channel

The **interfaceport-channel** command is now documented as the **port-channel**keyword of the **interface** command. For more information, see the **interface** command.

interface pos

The **interfacepos** command is now documented as the **pos**keyword of the **interface** command. For more information, see the **interface**command.

interface range

To execute commands on multiple subinterfaces at the same time, use the **interfacerange** command in global configuration mode.

interface range {*type number* [[**-interface** *number*]] [**,**] ... *type number* | **macro** *word*}
no interface range *type number*

Syntax Description

type number	Interface type and interface or subinterface number. For more information about the numbering syntax for your networking device, use the question mark (?) online help function. • You can enter any number of interface type and numbers.
- *interface-number*	(Optional) Ending interface number.
,	Allows you to configure more interface types.
macro	Specifies a macro keyword.
word	Previously defined keyword, up to 32 characters long.

Command Default

No interface range is set.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.0(7)XE	This command was introduced.
12.1(5)T	This command was integrated into Cisco IOS Release 12.1(5)T.
12.2(2)DD	This command was expanded to support subinterface ranges.
12.2(4)B	This command was integrated into Cisco IOS Release 12.2(4)B.
12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T.
12.2(18)SX	This command was integrated into Cisco IOS Release 12.2(18)SX.
12.2(33)SXH	The **create** keyword was added to enable the creation of VLANs that operate within a specified range of physical interfaces.

Usage Guidelines

Configuration Changes

All configuration changes made to a range of subinterfaces are saved to NVRAM, but the range itself does not get saved to NVRAM. Use the **defineinterfacerange** command to create and save a range.

You can enter the range in two ways:

- Specifying up to five interface ranges

- Specifying a previously defined macro

You can specify either the interfaces or the name of a range macro. A range must consist of the same interface type, and the interfaces within a range cannot span slots.

You cannot specify both the **interfacerange**and **macro** keywords in the same command. After creating a macro, the command does not allow you to enter additional ranges. Likewise, if you have already specified an interface range, the command does not allow you to enter a macro.

The spaces around the hyphen in the **interfacerange** command syntax are required. For example, using a Catalyst 6500 router, the command **interfacerangefastethernet1-6**is valid; the command **interfacerangefastethernet1-6**is not valid.

VLANs

When you define a Catalyst VLAN, valid values are from 1 to 4094. The last VLAN number cannot exceed 4094.

You cannot use the **interfacerange** command to create switch virtual interfaces (SVIs) in that particular range. You can use the **interfacerange** command only to configure existing VLAN SVIs within the range. To display VLAN SVIs, enter the **showrunning-config** command. VLANs not displayed cannot be used in the **interfacerange** command.

The commands entered under the**interfacerange** command are applied to all existing VLAN SVIs within the range.

You can enter the command **interfacerangecreatevlan***x-y* to create all VLANs in the specified range that do not already exist. If you are using discontiguous VLANs, you can use the **interfacerangevlan** command to configure multiple SVIs without creating unneeded SVIs and wasting interface descriptor blocks (IDBs).

After specifying a VLAN range, you can continue using the **interfacerange** command to specify another interface (**ATM**, **FastEthernet**, **GigabitEthernet**, **loopback**, **port-channel**, or **tunnel**).

Examples

interface range Fast Ethernet Examples

The following example shows how to use the **interfacerange** command to configure a Fast Ethernet range:

```
Router(config)# interface range fastethernet 5/1 - 4
```

The following example configures the Fast Ethernet subinterfaces within the range 5/1.1 to 5/1.4 and applies the following VLAN IDs to those subinterfaces:

```
Fast Ethernet5/1.1 = VLAN ID 301 (vlan-id)
Fast Ethernet5/1.2 = VLAN ID 302 (vlan-id = 301 + 2 - 1 = 302)
Fast Ethernet5/1.3 = VLAN ID 303 (vlan-id = 301 + 3 - 1 = 303)
Fast Ethernet5/1.4 = VLAN ID 304 (vlan-id = 301 + 4 - 1 = 304)
Router(config)# interface range fastethernet 5/1 - 4

Router(config-if-range)# encapsulation dot1q 301
Router(config-if-range)# no shutdown

Router(config-if)#
*Oct  6 08:24:35: %LINK-3-UPDOWN: Interface FastEthernet5/1.1, changed state to up
*Oct  6 08:24:35: %LINK-3-UPDOWN: Interface FastEthernet5/1.2, changed state to up
*Oct  6 08:24:35: %LINK-3-UPDOWN: Interface FastEthernet5/1.3, changed state to up
```

```
*Oct  6 08:24:35: %LINK-3-UPDOWN: Interface FastEthernet5/1.4, changed state to up
*Oct  6 08:24:36: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet5/1.1, changed
 state to up
*Oct  6 08:24:36: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet5/1.2, changed
 state to up
*Oct  6 08:24:36: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet5/1.3, changed
 state to up
*Oct  6 08:24:36: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet5/1.4, changed
 state to up
```

interface range Gigabit Ethernet Example

The following example shows how to set a Gigabit Ethernet range:

```
Router(config)# interface range gigabitethernet 1/1 - 6
```

interface range Loopback Example

The following example shows how to use the loopback interface:

```
Router(config)# interface range loopback 34567
```

interface range Tunnel Example

The following example shows how to use the tunnel interface:

```
Router(config)# interface range tunnel 55555
```

interface range Port Channel Example

The following example shows how to use the port-channel interface:

```
Router(config)# interface range port-channel 100
```

interface range VLAN Examples

The following example shows how to set a VLAN:

```
Router(config)# interface range vlan 123
```

The following example shows how to create a range of VLANs:

```
Router(config)# interface range create vlan 4
```

interface range macro Example

The following example shows how to execute a range macro:

```
Router(config)# interface range macro macro1
```

Related Commands

Command	Description
define interface range	Defines an interface range macro.
encapsulation dot1q	Applies a unique VLAN ID to each subinterface within the range.
interface vlan	Configures a VLAN interface.

interface satellite

To enter satellite interface configuration mode, use the **interfacesatellite** command in global configuration mode.

interface satellite *slot/unit*

Syntax Description

slot	Router chassis slot in which the network module is installed.
unit	Interface number. For NM-1VSAT-GILAT network modules, always use 0.

Command Default

No default behavior or values

Command Modes

Global configuration

Command History

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

Examples

The following example shows how to enter satellite interface configuration mode:

```
Router(config)# interface satellite 1/0

Router(config-if)#
```

Related Commands

Command	Description
service-module satellite status	Displays status information related to the hardware and software on the Cisco IP VSAT satellite WAN network module (NM-1VSAT-GILAT), including the initial configuration parameters.
show controllers satellite	Displays controller information about the internal router interface that connects to an installed Cisco IP VSAT satellite WAN network module (NM-1VSAT-GILAT).
show interface satellite	Displays general interface settings and traffic rates for the internal router interface that connects to an installed Cisco IP VSAT satellite WAN network module (NM-1VSAT-GILAT).

interface service-engine

To enter the interface configuration mode for a network module (NM) or an advanced Integration Module (AIM), use the **interfaceservice-engine** command in global configuration mode.

interface service-engine *slot/port*

Syntax Description

slot	Interface slot number.
port	Interface port number.

Command Default

No default behavior or values.

Command Modes

Global configuration

Command History

Release	Modification
12.2(15)ZJ	This command was introduced for NMs.
12.3(4)T	This command was integrated into Cisco IOS Release 12.3(4)T.
12.3(7)T	Support was added for AIMs.

Usage Guidelines

This command may only be used for NMs and AIMs. If your system does not have this hardware, then you will be unable to enter this command.

The **no** form of this command (**nointerfaceservice-engine**) is not available. The **exit** command can be used to exit the interface configuration mode.

Examples

The following example shows the command for entering configuration mode for either a NM or AIM located in slot 1, unit 1:

```
Router (config)# interface service-engine 1/1
Router (config-if)# exit
```

interface sm

To configure an interface on the router that connects to an SM-SRE service module, use the **interfacesm** command in global configuration mode. This command does not have a no form.

interface sm *slot*/*port*

Syntax Description

slot	Router slot in which the service module is installed. Range: 1 to 4.
/ *port*	Port number of the module interface. Range: 0 or 1. The slash mark (/) is required.

Command Default

The interface is not configured.

Command Modes

Global configuration (config)

Command History

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

Usage Guidelines

This command enters interface configuration mode to configure the interface between the router and the service module or between the service module and Multi-Gigabit Fabric (MGF).

Examples

The following example shows how to enter interface configuration mode for the service module:

```
Router(config)# interface sm 1/0
```

Related Commands

Command	Description
ip unnumbered	Enables IP processing on an interface without assigning an explicit IP address to the interface.
service-module ip address	Specifies the IP address of the module side of the interface.
show interfaces sm	Displays status, traffic data, and configuration information about the service module interface.

interface vg-anylan

The **interfacevg-anylan** command is now documented as the **vg-anylan** keyword of the **interface** command. For more information, see the **interface**command.

interface vmi

To create a virtual multipoint interface (VMI) that can be configured and applied dynamically, use the**interfacevmi** command in global configuration mode. To remove a VMI interface, use the **no** form of this command.

interface vmi *interface-number*
no interface vmi *interface-number*

Syntax Description

interface-number	Number assigned to the VMI. The value range for VMI interface numbers is from 1 to 2147483647

Command Default

No VMI is defined.

Command Modes

Global configuration (config)

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.

Usage Guidelines

VMI Interface Aggregation Point

The VMI interface acts as an aggregation point for multiple PPPoE connections from one or more radios over one or more physical interfaces.

OSPFv3 and EIGRP Route Advertisements

All OSPFv3, EIGRPv4, and EIGRPv6 route advertisements that are received over the PPPoE connections are reported to the routing protocol as coming from a single interface, thus simplifying the routing protocol topology table and providing scalability benefits of each of the routing protocols.

Examples

The following example shows how to create a VMI interface:

```
interface vmi 1
 ip address 10.2.1.1 255.255.255.0
 no ip redirects
 no ip split-horizon eigrp 1
 load-interval 30
 ipv6 address 2001:0DB8:1:1:FFFF:FFFF:FFFF:FFFE/64
 ipv6 enable
 no ipv6 redirects
 ipv6 eigrp 1
 no ipv6 split-horizon eigrp 1
 physical-interface GigabitEthernet 0/0
 end
```

Related Commands

Command	Description
debug vmi	Displays debugging output for virtual multipoint interfaces (VMIs).

Command	Description
eigrp interface	Sets a threshold value to minimize hysteresis in a router-to-radio configuration.
mode bypass	Enables virtual multipoint interfaces (VMIs) to support multicast traffic.
physical interface	Creates a physical subinterface to be associated with the virtual multipoint interfaces (VMIs) on a router.

interface wlan-controller

To configure the Cisco Wireless Local Area Network (WLAN) controller network module interface with dot1q encapsulation on the router, use the **interfacewlan-controller** command in global configuration mode.

interface wlan-controller slot/unit

Syntax Description

slot/unit	Specifies the router slot and unit numbers for the WLAN controller network module.

Command Default

None

Command Modes

Global configuration

Command History

Release	Modification
12.4(2)XA1	This command was introduced on the router software.
12.4(6)T	This command was integrated into Cisco IOS Release 12.4(6)T.

Examples

The following example shows how to create dot1Q virtual LAN (VLAN) subinterfaces under interface wlan-controller:

```
Router(config)# interface wlan-controller 1/0
Router(config-if)# exit
Router(config)# interface wlan-controller 1/0.10
Router(config-subif)# encapsulation dot1q 10

If the interface doesn't support baby giant frames
maximum mtu of the interface has to be reduced by 4
bytes on both sides of the connection to properly
transmit or receive large packets. Please refer to
documentation on configuring IEEE 802.1Q vLANs.

Router(config-subif)# end
```

international bit

To set the E3 international bit in the G.751 frame used by the PA-E3 port adapter, use the **internationalbit**command in interface configuration mode. To return to the default international bit, use the **no** form of this command.

international bit commandinternational bit {**0** | **1**} {**0** | **1**}
no international bit

Syntax Description

0	Sets either of the two required E3 international bits in the G.751 frame to 0. This is the default.
1	Sets either of the two required E3 international bits in the G.751 frame to 1.

Command Default

The default value for each bit is 0.

Command Modes

Interface configuration

Command History

Release	Modification
11.1 CA	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

The **internationalbit** command sets bits 6 and 8, respectively, of set II in the E3 frame.

To verify the international bit configured on the interface, use the **showcontrollersserial** EXEC command.

Examples

The following example sets the international bit to 1 1 on the PA-E3 port adapter in slot 1, port adapter slot 0, interface 0:

```
Router(config)# interface serial 1/0/0
Router(config-if)# international bit 1 1
```

Related Commands

Command	Description
national bit (interface)	Sets the E3 national bit in the G.751 frame used by the PA-E3 port adapter.
show controllers serial	Displays information that is specific to the interface hardware.

inter-packet gap 6502-mode

To set the Inter-Packet Gap (IPG) value, use the **inter-packetgap6502-mode**command in interface configuration mode. To return to the default setting, use the **no** form of this command.

inter-packet gap 6502-mode
no inter-packet gap 6502-mode

Syntax Description

This command has no keywords or arguments.

Command Default

All fragments from flows that are received from an ACE with Layer 4 ports and permit action are permitted. All other fragments are dropped in the hardware. This action also applies to flows that are handled in the software regardless of this command setting.

Command Modes

Interface configuration

Command History

Release	Modification
12.2(18)SXF5	This command was introduced on the Supervisor Engine 720.

Usage Guidelines

This command is supported only when a WS-X6704-10GE is connected to a WS-X6502-10GE. You enter this command to change the IPG value of the WS-X6704-10GE to match the IPG value of the WS-X6502-10GE.

The default 6704 mode sets the IPG value to average 12. Based on packet size, the IPG between successive packets ranges from 9 to 15.

The 6502 mode sets the IPG value to average 16. Based on packet size, the IPG between successive packets ranges from 13 to 19.

Examples

This example shows how to set the IPG to 6502 mode:

```
inter-packet gap 6502-mode
```

This example shows how to set the IPG to the default mode:

```
no inter-packet gap 6502-mode
```

invert data

To invert the data stream, use the **invertdata** command in interface configuration mode. This command applies only to the Cisco 7000 series routers with the RSP7000 and RSP7000CI, Cisco 7200 series routers, and Cisco 7500 series routers. To disable inverting the data stream, use the **no** form of this command.

invert data commandinvert data
no invert data

Syntax Description

This command has no arguments or keywords.

Command Default

Data is not inverted.

Command Modes

Interface configuration

Command History

Release	Modification
11.1CA	This command was introduced.
11.2P	This command was integrated into Cisco IOS Release 11.2 P.
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

T1 Line Without B8ZS Encoding

If the interface on the PA-8T and PA-4T+ synchronous serial port adapters and the PA-T3 and PA-2T3 synchronous serial port adapters is used to drive a dedicated T1 line that does not have B8ZS encoding (a method to avoid 15 zeros), the data stream must be inverted (both transmitting and receiving data) either in the connecting CSU/DSU or in the interface.

Inverting is a method of avoiding excessive zeroes that is superseded by the use of B8ZS encryption. This option could be needed for use with legacy equipment that supports this option. By inverting the High-Level Data Link Control (HDLC) data stream, the HDLC zero insertion algorithm becomes a ones insertion algorithm that satisfies the T1 requirements. Be careful not to invert data both on the interface and on the CSU/DSU because two data inversions will cancel each other out.

AMI Line Coding

If the interface on the CT3IP uses alternate mark inversion (AMI) line coding, you must also invert the data on the T1 channel. For more information, see the **t1linecode**controller configuration command.

Examples

The following example inverts data on serial interface 3/1/0:

```
Router(config)# interface serial 3/1/0
Router(config-if)# invert data
```

Related Commands

Command	Description
t1 linecode	Specifies the type of linecoding used by the T1 channels on the CT3IP in Cisco 7500 series routers.

invert rxclock

To invert the phase of the receive (RX) clock signal on the universal I/O (UIO) serial interface that does not use the T1/E1 interface, use the **invertrxclock** command in interface configuration mode. To disable the phase inversion, use the **no** form of this command.

invert rxclock commandinvert rxclock
no invert rxclock

Syntax Description

This command has no arguments or keywords.

Command Default

The receive clock signal is not inverted.

Command Modes

Interface configuration

Command History

Release	Modification
11.3 MA	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

When a delay occurs between a signal being sent and the signal being received it can indicate that the receive clock signal is not appropriate for the interface rate. This command allows the receive clock signal to be inverted to attempt to correct the delay.

Examples

The following example inverts the receive clock signal on serial interface 1:

```
Router(config)# interface serial 1
Router(config-if)# invert rxclock
```

invert txclock

To invert the transmit (TX) clock signal, use the **inverttxclock** command in interface configuration mode. To return the TX clock signal to its initial state, use the **no** form of this command.

invert txclock
no invert txclock

Syntax Description

This command has no arguments or keywords.

Command Default

The transmit clock signal is not inverted.

Command Modes

Interface configuration

Command History

Release	Modification
10.0	This command was introduced.
11.3	The **invert-transmit-clock** command was replaced by the **inverttxclock** command.
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

Delays between the serial clock transmit external (SCTE) clock and data transmission indicate that the TX clock signal might not be appropriate for the interface rate and length of cable being used. Different ends of the wire can have variances that differ slightly. The **inverttxclock** command compensates for these variances. This command replaces the **invert-transmit-clock** command.

Systems that use long cables or cables that are not transmitting the TxC signal (transmit echoed clock line, also known as TXCE or SCTE clock) can experience high error rates when operating at the higher transmission speeds. For example, if a PA-8T synchronous serial port adapter is reporting a high number of error packets, a phase shift might be the problem. Inverting the clock might correct this shift.

When a PA-8T or PA-4T+ port adapter interface is DTE, the **inverttxclock**command inverts the TxC signal it received from the remote DCE. When the PA-8T or PA-4T+ port adapter interface is DCE, this command changes the signal back to its original phase.

Examples

The following example inverts the TX clock signal on serial interface 3/0:

```
Router(config)# interface serial 3/0
Router(config-if)# invert txclock
```

ip dscp

To enable the use of IP differentiated services code point (DSCP) for packets that originate from a circuit emulation (CEM) channel, use the **ipdscp** command in CEM configuration mode. To disable the use of IP DSCP, use the **no** form of this command.

ip dscp [*dscp-value*]
no ip dscp

Syntax Description

dscp-value	(Optional) Value placed in the DSCP field of IP packets that originate from a CEM channel. Range is from 0 to 63. Default is 46.

Command Default

IP DSCP is enabled for packets that originate from a CEM channel.

Command Modes

CEM configuration

Command History

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

Usage Guidelines

DSCP is mutually exclusive from both IP type of service (ToS) and IP precedence. Thus, if DSCP is configured, the **iptos** command and the **ipprecedence** command are both unavailable at the command-line interface (CLI).

Examples

The following example shows how to set the IP DSCP field value to 36.

```
Router(config-cem)# ip dscp 36
```

Related Commands

Command	Description
ip precedence	Configures the IP precedence bits for the CEM channel.
ip tos	Configures the IP ToS bits for the CEM channel.

ip pxf

To manually enable the PXF processors, use the **ippxf** command in global configuration mode. To manually disable the PXF processors, use the **no** form of this command.

ip pxf
no ip pxf

Syntax Description

This command has no arguments or keywords.

Command Default

The PXF processors are enabled by default.

Command Modes

Global configuration

Command History

Release	Modification
12.1(9)EX	This command was introduced.
12.2(18)S	This command was introduced on Cisco 7304 routers running Cisco IOS Release 12.2(18)S.
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

The PXF processors are enabled by default. If they are ever disabled, you must enable them to take advantage of IP packet switching and feature acceleration. The PXF processors should never be disabled except for very short durations for debugging purposes.

Note You must also have IP Cisco Express Forwarding switching turned on for accelerated IP packet switching.

Examples

The following example enables the PXF processors:

```
ip pxf
```

Related Commands

Command	Description
show c7300 pxf accounting	Displays the number of packets entering or exiting the PXF processors.
show pxf accounting	Displays the PXF accounting.
show c7300 pxf interfaces	Displays the status of various interfaces known to the PXF processors.
show pxf interfaces	Displays a list of PXF interfaces.

ip rbscp ack-split

To configure the TCP ACK splitting feature of the Rate-Based Satellite Control Protocol (RBSCP) on an outgoing interface for packets that are permitted by a specified access list, use the **iprbscpack-split**command in interface configuration mode. To disable the feature on the interface, use the **no** form of this command.

ip rbscp ack-split *size* {*access-list-nameaccess-list-number*} **out**
no ip rbscp ack-split

Syntax Description

size	The number of TCP ACKs to send for every TCP ACK received. A *size*of 0 or 1 indicates that this feature is disabled (that is, no TCP ACK splitting will occur). The range is 0 through 32.
access-list-name | *access-list-number*	Standard or extended IP access list name or number that controls which packets are subject to TCP ACK splitting. That is, the feature is applied to packets that a **permit** statement allows; the feature is not applied to packets that a **deny** statement filters.
out	Specifies that this feature is applied to an outgoing interface.

Command Default

Disabled (TCP ACK splitting is not required on an outgoing interface for packets that are permitted by a specified acccess list).

Command Modes

Interface configuration

Command History

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

Usage Guidelines

This command enables TCP ACK splitting for outgoing packets that are permitted by the access list. TCP ACK splitting is a software technique to improve performance for clear-text TCP traffic using acknowledgment (ACK) splitting, in which a number of additional TCP ACKs are generated for each TCP ACK received.

TCP ACK splitting causes TCP to open the congestion window more quickly than usual, thus decreasing the effect of long latencies. TCP will generally open the congestion window by one maximum transmission unit (MTU) for each TCP ACK received. Opening the congestion window results in increased bandwidth becoming available. Configure this feature only when the satellite link is not using all the available bandwidth. Encrypted traffic cannot use TCP ACK splitting.



Caution Plan your network carefully so that no more than one Cisco IOS router in a given routing path has this feature enabled. You do not want to recursively ACK-split traffic.

An interface can use only one instance of this feature at a time. Each instance of this feature can be used on multiple interfaces.

If you configure this feature but it refers to a nonexistent access list, this is interpreted as having an access list that denies all traffic from being processed by the Access-List-Based RBSCP feature, so the feature is essentially disabled and the traffic goes through the normal switching path.

Examples

In the following example, the access list performs TCP ACK splitting on packets going out Ethernet interface 0 from a source at 172.22.18.5 to a destination at 172.23.27.4:

```
ip access-list extended satellite
 permit tcp 172.22.18.5 172.23.27.4
 exit
interface ethernet 0
 ip rbscp ack-split 6 satellite out
```

Related Commands

Command	Description
debug ip rbscp	Displays general error messages about access-list-based RBSCP.
debug ip rbscp ack-split	Displays information about TCP ACK splitting done in conjunction with RBSCP.

ip verify unicast source reachable-via

To enable Unicast Reverse Path Forwarding (Unicast RPF), use the **ip verify unicast source reachable-via** command in interface configuration mode. To disable Unicast RPF, use the **no** form of this command.

ip verify unicast source reachable-via {**any** | **rx** [**l2-src**]} [**allow-default**] [**allow-self-ping**] [*access-list*]
no ip verify unicast source reachable-via

Syntax Description

any	Examines incoming packets to determine whether the source address is in the Forwarding Information Base (FIB) and permits the packet if the source is reachable through any interface (sometimes referred to as loose mode).
rx	Examines incoming packets to determine whether the source address is in the FIB and permits the packet only if the source is reachable through the interface on which the packet was received (sometimes referred to as strict mode).
l2-src	(Optional) Enables source IPv4 and source MAC address binding.
allow-default	(Optional) Allows the use of the default route for RPF verification.
allow-self-ping	(Optional) Allows a router to ping its own interface or interfaces. **Caution** Use caution when enabling the **allow-self-ping** keyword. This keyword opens a denial-of-service (DoS) hole.
access-list	(Optional) Specifies a numbered access control list (ACL) in the following ranges: • 1 to 99 (IP standard access list) • 100 to 199 (IP extended access list) • 1300 to 1999 (IP standard access list, expanded range) • 2000 to 2699 (IP extended access list, expanded range)

Command Default

Unicast RPF is disabled.

Source IPv4 and source MAC address binding is disabled.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
11.1(CC), 12.0	This command was introduced. This command was not included in Cisco IOS Release 11.2 or 11.3.
12.1(2)T	Added access control list (ACL) support using the *access-list* argument. Added per-interface statistics on dropped or suppressed packets.

Release	Modification
12.0(15)S	This command replaced the **ip verify unicast reverse-path** command, and the following keywords were added: **allow-default**, **allow-self-ping**, **rx**, and **any**.
12.1(8a)E	This command was integrated into Cisco IOS Release 12.1(8a)E.
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 introduced on the Supervisor Engine 720.
12.2(17d)SXB	Support for this command was introduced on the Supervisor Engine 2.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SRC	This command was modified. The **l2-src** keyword was added to support the source IPv4 and source MAC address binding feature on platforms that support the Cisco Express Forwarding software switching path.
15.0(1)M	This command was integrated into Cisco IOS Release 15.0(1)M.

Usage Guidelines

Use the **ip verify unicast source reachable-via** interface command to mitigate problems caused by malformed or forged (spoofed) IP source addresses that pass through a router. Malformed or forged source addresses can indicate DoS attacks based on source IP address spoofing.

To use Unicast RPF, enable Cisco Express Forwarding or distributed Cisco Express Forwarding in the router. There is no need to configure the input interface for Cisco Express Forwarding. As long as Cisco Express Forwarding is running on the router, individual interfaces can be configured with other switching modes.



Note It is important for Cisco Express Forwarding to be configured globally on the router. Unicast RPF does not work without Cisco Express Forwarding.



Note Unicast RPF is an input function and is applied on the interface of a router only in the ingress direction.

When Unicast RPF is enabled on an interface, the router examines all packets that are received on that interface. The router checks to make sure that the source address appears in the FIB. If the **rx** keyword is selected, the source address must match the interface on which the packet was received. If the **any** keyword is selected, the source address must be present only in the FIB. This ability to "look backwards" is available only when Cisco Express Forwarding is enabled on the router because the lookup relies on the presence of the FIB. Cisco Express Forwarding generates the FIB as part of its operation.



Note If the source address of an incoming packet is resolved to a null adjacency, the packet will be dropped. The null interface is treated as an invalid interface by the new form of the Unicast RPF command. The older form of the command syntax did not exhibit this behavior.

Unicast RPF checks to determine whether any packet that is received at a router interface arrives on one of the best return paths to the source of the packet. If a reverse path for the packet is not found, Unicast RPF can drop or forward the packet, depending on whether an ACL is specified in the Unicast RPF command. If an ACL is specified in the command, when (and only when) a packet fails the Unicast RPF check, the ACL is checked to determine whether the packet should be dropped (using a deny statement in the ACL) or forwarded (using a permit statement in the ACL). Whether a packet is dropped or forwarded, the packet is counted in the global IP traffic statistics for Unicast RPF drops and in the interface statistics for Unicast RPF.

If no ACL is specified in the **ip verify unicast source reachable-via** command, the router drops the forged or malformed packet immediately, and no ACL logging occurs. The router and interface Unicast RPF counters are updated.

Unicast RPF events can be logged by specifying the logging option for the ACL entries that are used by the **ip verify unicast source reachable-via** command. Log information can be used to gather information about the attack, such as source address, time, and so on.

Strict Mode RPF

If the source address is in the FIB and reachable only through the interface on which the packet was received, the packet is passed. The syntax for this method is **ip verify unicast source reachable-via rx**.

Exists-Only (or Loose Mode) RPF

If the source address is in the FIB and reachable through any interface on the router, the packet is passed. The syntax for this method is **ip verify unicast source reachable-via any**.

Because this Unicast RPF option passes packets regardless of which interface the packet enters, it is often used on Internet service provider (ISP) routers that are "peered" with other ISP routers (where asymmetrical routing typically occurs). Packets using source addresses that have not been allocated on the Internet, which are often used for spoofed source addresses, are dropped by this Unicast RPF option. All other packets that have an entry in the FIB are passed.

allow-default

Normally, sources found in the FIB but only by way of the default route will be dropped. Specifying the **allow-default** keyword option will override this behavior. You must specify the **allow-default** keyword in the command to permit Unicast RPF to successfully match on prefixes that are known through the default route to pass these packets.

allow-self-ping

This keyword allows the router to ping its own interface or interfaces. By default, when Unicast RPF is enabled, packets that are generated by the router and destined to the router are dropped, thereby, making certain troubleshooting and management tasks difficult to accomplish. Issue the **allow-self-ping** keyword to enable self-pinging.



Caution Caution should be used when enabling the **allow-self-ping** keyword because this option opens a potential DoS hole.

Using RPF in Your Network

Use Unicast RPF strict mode on interfaces where only one path allows packets from valid source networks (networks contained in the FIB). Also, use Unicast RPF strict mode when a router has multiple paths to a given network, as long as the valid networks are switched through the incoming interfaces. Packets for invalid networks will be dropped. For example, routers at the edge of the network of an ISP are likely to have

symmetrical reverse paths. Unicast RPF strict mode is applicable in certain multihomed situations, provided that optional Border Gateway Protocol (BGP) attributes, such as weight and local preference, are used to achieve symmetric routing.



Note With Unicast RPF, all equal-cost "best" return paths are considered valid. This means that Unicast RPF works in cases where multiple return paths exist, provided that each path is equal to the others in terms of the routing cost (number of hops, weights, and so on) and as long as the route is in the FIB. Unicast RPF also functions where Enhanced Internet Gateway Routing Protocol (EIGRP) variants are being used and unequal candidate paths back to the source IP address exist.

Use Unicast RPF loose mode on interfaces where asymmetric paths allow packets from valid source networks (networks contained in the FIB). Routers that are in the core of the ISP network have no guarantee that the best forwarding path out of the router will be the path selected for packets returning to the router.

IP and MAC Address Spoof Prevention

In Release 15.0(1)M and later, you can use the **l2-src**keyword to enable source IPv4 and source MAC address binding. To disable source IPv4 and source MAC address binding, use the **no** form of the **ip verify unicast source reachable-via**command.

If an inbound packet fails this security check, it will be dropped and the Unicast RPF dropped-packet counter will be incremented. The only exception occurs if a numbered access control list has been specified as part of the Unicast RPF command in strict mode, and the ACL permits the packet. In this case the packet will be forwarded and the Unicast RPF suppressed-drops counter will be incremented.



Note The **l2-src** keyword cannot be used with the loose uRPF command, **ip verify unicast source reachable-via any**command.

Not all platforms support the **l2-src** keyword. Therefore, not all the possible keyword combinations for strict Unicast RPF in the following list will apply to your platform:

Possible keyword combinations for strict Unicast RPF include the following:

```
allow-default
allow-self-ping
l2-src
<ACL-number>
allow-default allow-self-ping
allow-default l2-src
allow-default <ACL-number>
allow-self-ping l2-src
allow-self-ping <ACL-number>
l2-src <ACL-number>
allow-default allow-self-ping l2-src
allow-default allow-self-ping <ACL-number>
allow-default l2-src <ACL-number>
allow-self-ping l2-src <ACL-number>
allow-default allow-self-ping l2-src <ACL-number>
```

Examples

Single-Homed ISP Connection with Unicast RPF

The following example uses a very simple single-homed ISP connection to demonstrate the concept of Unicast RPF. In this example, an ISP peering router is connected through a single serial interface to one upstream ISP. Hence, traffic flows into and out of the ISP will be symmetric. Because traffic flows will be symmetric, a Unicast RPF strict-mode deployment can be configured.

```
ip cef
! or "ip cef distributed" for Route Switch Processor+Versatile Interface Processor-
(RSP+VIP-) based routers.
!
interface Serial5/0/0
 description - link to upstream ISP (single-homed)
 ip address 192.168.200.225 255.255.255.252
 no ip redirects
 no ip directed-broadcasts
 no ip proxy-arp
 ip verify unicast source reachable-via
```

ACLs and Logging with Unicast RPF

The following example demonstrates the use of ACLs and logging with Unicast RPF. In this example, extended ACL 197 provides entries that deny or permit network traffic for specific address ranges. Unicast RPF is configured on interface Ethernet 0/1/1 to check packets arriving at that interface.

For example, packets with a source address of 192.168.201.10 arriving at interface Ethernet 0/1/1 are dropped because of the deny statement in ACL 197. In this case, the ACL information is logged (the logging option is turned on for the ACL entry) and dropped packets are counted per-interface and globally. Packets with a source address of 192.168.201.100 arriving at interface Ethernet 0/1/2 are forwarded because of the permit statement in ACL 197. ACL information about dropped or suppressed packets is logged (the logging option is turned on for the ACL entry) to the log server.

```
ip cef distributed
!
int eth0/1/1
 ip address 192.168.200.1 255.255.255.0
 ip verify unicast source reachable-via rx 197
!
int eth0/1/2
 ip address 192.168.201.1 255.255.255.0
!
access-list 197 deny   ip 192.168.201.0 0.0.0.63 any log-input
access-list 197 permit ip 192.168.201.64 0.0.0.63 any log-input
access-list 197 deny   ip 192.168.201.128 0.0.0.63 any log-input
access-list 197 permit ip 192.168.201.192 0.0.0.63 any log-input
access-list 197 deny ip host 0.0.0.0 any log-input
access-list 197 deny ip 172.16.0.0 0.255.255.255 any log-input
access-list 197 deny ip 10.0.0.0 0.255.255.255 any log-input
access-list 197 deny ip 172.16.0.0 0.15.255.255 any log-input
access-list 197 deny ip 192.168.0.0 0.0.255.255 any log-input
```

MAC Address Binding on Software Switching Platforms Like the Cisco 7200 Series Routers

The following example shows how to enable source IPv4 and source MAC address binding on Ethernet 0/0:

```
Router# configure terminal
Router(config)# interface Ethernet0/0
Router(config-if)# ip address 10.0.0.1 255.255.255.0
Router(config-if)# ip verify unicast source reachable-via rx l2-src
```

Related Commands

Command	Description
ip cef	Enables Cisco Express Forwarding on the route processor card.
ip cef distributed	Enables Cisco Express Forwarding on the line card.

ipc buffers

To resize the interprocessor communication (IPC) buffer pool, use the **ipcbuffers** command in global configuration mode. To disable the configuration, use the **no** form of this command.

ipc buffers {**max-free** | **min-free** | **permanent**} *buffers*
no ipc buffers {**max-free** | **min-free** | **permanent**}

Syntax Description

max-free *buffers*	Specifies the maximum number of buffers that must be free. The range is from 8 to 10000.
min-free *buffers*	Specifies the minimum number of buffers that must be free. The range is from 1 to 17.
permanent *buffers*	Specifies the number of buffers that must be permanantly allocated for IPC apart from the buffers that are dynamically allocated and freed. The range is from 2 to 5000.

Command Default

The default buffer value is set by the platform during initialization.

Command Modes

Global configuration (config)

Command History

Release	Modification
15.0(1)M	This command was introduced in a release earlier than Cisco IOS Release 15.0(1)M.
Cisco IOS XE Release 2.1	This command was implemented on the Cisco ASR 1000 Series Aggregation Services Routers.

Usage Guidelines

You can use the **ipcbuffers** command when you would want to resize the buffer pool.

Examples

The following example shows how to set the maximum number of free buffers to 10:

```
Router(config)# ipc buffers max-free 10
```

Related Commands

Command	Description
ipc holdq threshold	Configures IPC holdq threshold values.
show ipc	Displays IPC statistics.

ipc header-cache

To resize the interprocess communication (IPC) permanent cache, use the **ipcheader-cache** command in global configuration mode. To disable the configuration, use the **no** form of this command.

ipc header-cache permanent *high-cache low-cache*
no ipc header-cache permanent

Syntax Description

permanent	Specifies the permanent IPC cache.
high-cache	Maximum permanent cache size. The range is from 1000 to 10000.
low-cache	Lower cache watermark. The range is from 100 to 2000.

Command Default

The default values are set by the platform during initialization.

Command Modes

Global configuration (config)

Command History

Release	Modification
15.0(1)M	This command was introduced in a release earlier than Cisco IOS Release 15.0(1)M.
Cisco IOS XE Release 2.1	This command was implemented on the Cisco ASR 1000 Series Aggregation Services Routers.

Examples

The following example shows how to set the maximum permanent cache value to 1000 and lower cache value to 200 of an IPC server:

```
Router(config)# ipc header-cache permanent 1000 200
```

Related Commands

Command	Description
ipc holdq threshold	Configures IPC holdq threshold values.
show ipc	Displays IPC statistics.

ipc holdq threshold

To configure interprocessor communication (IPC) holdq threshold values, use the **ipcholdqthreshold**command in global configuration mode. To disable the configuration, use the **no** form of this command.

ipc holdq threshold {**lower** *start-threshold* | **upper** *stop-threshold*}
no ipc holdq threshold {**lower** | **upper**}

Syntax Description

lower	Specifies the lower threshold for IPC holdq.
start-threshold	Threshold to start sending IPC messages. The range is from 10 to 2000.
upper	Specifies the upper threshold for IPC holdq.
stop-threshold	Threshold to stop sending IPC messages. The range is from 40 to 4000.

Command Default

The default values threshold is set by the platform during initialization.

Command Modes

Global configuration (config)

Command History

Release	Modification
15.0(1)M	This command was introduced in a release earlier than Cisco IOS Release 15.0(1)M.
12.2(33)SXI	This command was integrated into a release earlier than Cisco IOS Release 12.2(33)SXI.
Cisco IOS XE Release 2.1	This command was implemented on the Cisco ASR 1000 Series Aggregation Services Routers.

Usage Guidelines

The holdq OFF and ON thresholds are used to throttle the message sent based on the traffic at the driver. If the number of messages to be processed by the driver has increased than the OFF threshold, then the messages are not passed from the transport layer to the driver. The messages will be sent again once the count decreases below the ON threshold.

You can use the**ipcholdq**command when the driver message processing speed has decreased or increased to a greater extent than the specifications.

Examples

The following example shows how to configure a lower threshold value of 100 for IPC holdq:

```
Router(config)# ipc holdq threshold lower 100
```

Related Commands

Command	Description
ipc buffers	Resizes the IPC buffer pool.
show ipc	Displays IPC statistics.

ipc master

To configure the IP address of the interprocessor communication (IPC) master server, use the **ipcmaster** command in global configuration mode. To disable the configuration, use the **no** form of this command.

ipc master {*ip-address* | **self**}
no ipc master

Syntax Description

ip-address	IP address of the master server.
self	Assigns the host as the IPC master server.

Command Default

IP address is not configured.

Command Modes

Global configuration (config)

Command History

Release	Modification
15.0(1)M	This command was introduced in a release earlier than Cisco IOS Release 15.0(1)M.

Examples

The following example shows how to configure 192.0.2.1 as the IP address of the master server:

```
Router(config)# ipc master 192.0.2.1
```

Related Commands

Command	Description
ipc buffers	Resizes the IPC buffer pool.
show ipc	Displays IPC statistics.

ipc zone default

To enter interprocess communication (IPC) zone configuration mode, use the **ipczonedefault**command in global configuration mode. To remove a previously configured association, use the **no** form of this command.

ipc zone default
no ipc zone default

Syntax Description

This command has no arguments or keywords.

Command Default

The user is not in IPC zone configuration mode.

Command Modes

Global configuration

Command History

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

Usage Guidelines

The **ipczonedefault** command places the router into IPC zone configuration mode. In this mode, the user can configure the default IPC zone.

The **no** form of the **ipczonedefault** command removes any previously configured association.

Examples

The following example places the router into IPC zone configuration mode:

```
Router(config)# ipc zone default
Router(config-ipczone)#
```

Related Commands

Command	Description
show ipc	Displays IPC statistics.

iphc-profile

To create an IP Header Compression (IPHC) profile and to enter IPHC-profile configuration mode, use the **iphc-profile** command in global configuration mode. To attach an existing IPHC profile to an interface or subinterface, use the **iphc-profile** command in interface configuration mode. To delete the IPHC profile, use the **no** form of this command.

iphc-profile *profile-name* {**ietf** | **van-jacobson**}
no iphc-profile *profile-name*

Syntax Description

profile-name	Name of the IPHC profile to be created or attached. The IPHC profile name can be a maximum of 32 characters. The name may not include quotation marks, white space, or special characters.
ietf	Specifies that the IPHC profile is for Internet Engineering Task Force (IETF) header compression.
van-jacobson	Specifies that the IPHC profile is for Van Jacobson header compression.

Command Default

No IPHC profile is created or attached.

Command Modes

Global configuration (to create an IPHC profile) Interface configuration (to attach an existing IPHC profile to an interface or subinterface)

Command History

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

Usage Guidelines

The **iphc-profile** command creates an IPHC profile used for enabling header compression and enters IPHC-profile configuration mode (config-iphcp). An IPHC profile is a template within which you can configure the type of header compression that you want to use, enable any optional features and settings for header compression, and then apply the profile to an interface, a subinterface, or a Frame Relay permanent virtual circuit (PVC).

Specifying the IPHC Profile Type

When you create an IPHC profile, you must specify the IPHC profile type by using either the **ietf** keyword or the **van-jacobson** keyword. The IETF profile type conforms to and supports the standards established with RFC 2507, RFC 2508, RFC 3544, and RFC 3545 and is typically associated with non-TCP header compression (for example, RTP header compression). The Van Jacobson profile type conforms to and supports the standards established with RFC 1144 and is typically associated with TCP header compression.

Note If you are using Frame Relay encapsulation, you must specify the **ietf**keyword (not the **van-jacobson** keyword).

Considerations When Specifying the IPHC Profile Type

When specifying the IPHC profile type, consider whether you are compressing TCP traffic or non-TCP traffic (that is, RTP traffic). Also consider the header compression format capabilities of the remote network link

that will receive traffic. The IPHC profile type that you specify directly affects the header compression format used on the remote network links to which the IPHC profile is applied. *Only* TCP traffic is compressed on remote network links using a Van Jacobson IPHC profile, whereas TCP *and/or* non-TCP traffic (for example, RTP traffic) is compressed on remote network links using an IETF IPHC profile.



Note The header compression format in use on the router that you are configuring and the header compression format in use on the remote network link must match.

Configurable Header Compression Features and Settings

The specific set of header compression features and settings that you can configure (that is, enable or modify) is determined by the IPHC profile type that you specify (either IETF or Van Jacobson) when you create the IPHC profile. Both sets are listed below.

If you specify Van Jacobson as the IPHC profile type, you can enable TCP header compression and set the number of TCP contexts. The table below lists each available Van Jacobson IPHC profile type header compression feature and setting and the command used to enable it.

Table 4: Van Jacobson IPHC Profile Type Header Compression Features and Settings

Command	Feature or Setting
tcp	Enables TCP header compression.
tcp contexts	Sets the number of contexts available for TCP header compression.

If you specify IETF as the IPHC profile type, you can enable non-TCP header compression (that is, RTP header compression), along with a number of additional features and settings. The table below lists each available IETF IPHC profile type header compression feature and setting and the command or commands used to enable it.

Table 5: IETF IPHC Profile Type Header Compression Features and Settings

Command	Feature or Setting
feedback	Enables the context-status feedback messages from the interface or link.
maximum header	Sets the maximum size of the compressed IP header.
non-tcp	Enables non-TCP header compression.
non-tcp contexts	Sets the number of contexts available for non-TCP header compression.
rtp	Enables RTP header compression.
recoverable-loss	Enables Enhanced Compressed Real-Time Transport Protocol (ECRTP) on an interface.
refresh max-period refresh max-time refresh rtp	Sets the context refresh (full-header refresh) options, such as the amount of time to wait before a full header is refreshed.

Command	Feature or Setting
tcp	Enables TCP header compression.
tcp contexts	Sets the number of contexts available for TCP header compression.

For More Information About IPHC Profiles

For more information about using IPHC profiles to configure header compression, see the "Header Compression" module and the "Configuring Header Compression Using IPHC Profiles" module of the Cisco IOS Quality of Service Solutions Configuration Guide, Release 12.4T.

Examples

In the following example, an IPHC profile called profile1 is created, and the Van Jacobson IPHC profile type is specified.

```
Router> enable
Router# configure terminal
Router(config)# iphc-profile profile1 van-jacobson
Router(config-iphcp)# end
```

In the following example, a second IPHC profile called profile2 is created. For this IPHC profile, the IETF IPHC profile type is specified.

```
Router> enable
Router# configure terminal
Router(config)# iphc-profile profile2 ietf
Router(config-iphcp)# end
```

In the following example, an existing IPHC profile called profile2 is attached to serial interface 3/0. For this IPHC profile, the IPHC profile type (in this case, IETF) of profile2 is specified.

```
Router> enable
Router# configure terminal
Router(config)# interface serial 3/0
Router(config-if)# iphc-profile profile2 ietf
Router(config-iphcp)# end
```

Related Commands

Command	Description
feedback	Enables the context-status feedback messages from the interface or link.
maximum header	Specifies the maximum size of the compressed IP header.
non-tcp	Enables non-TCP header compression within an IPHC profile.
non-tcp contexts	Sets the number of contexts available for non-TCP header compression.
recoverable-loss	Enables ECRTP on an interface.
refresh max-period	Sets the number of packets sent between full-header refresh occurrences.
refresh max-time	Sets the amount of time to wait before a full-header refresh occurrence.
refresh rtp	Enables a context refresh occurrence for RTP header compression.

Command	Description
rtp	Enables RTP header compression within an IPHC profile.
show iphc-profile	Displays configuration information for one or more IPHC profiles.
tcp	Enables TCP header compression within an IPHC profile.
tcp contexts	Set the number of contexts available for TCP header compression.

keepalive

To enable keepalive packets and to specify the number of times that the Cisco IOS software tries to send keepalive packets without a response before bringing down the interface or before bringing down the tunnel protocol for a specific interface, use the **keepalive** command in interface configuration mode. When the keepalive function is enabled, a keepalive packet is sent at the specified time interval to keep the interface active. To turn off keepalive packets entirely, use the **no** form of this command.

keepalive [*period*[**retries**]]
no keepalive [*period*[**proto-up**]]

Syntax Description

period	(Optional) Integer value that represents the time interval, in seconds, between messages sent by the Cisco IOS software to ensure that a network interface is alive. • The valid range is from 0 to 32767 and the default value is 10.
retries	(Optional) Number of times that the device will continue to send keepalive packets without a response before bringing the interface down. • The valid range is 2 to 244. If omitted, the value that was previously set is used; if no value was specified, the default of 5 is used. • If this command is used with a tunnel interface, this argument value specifies the number of times that the device will continue to send keepalive packets without a response before bringing down the tunnel interface protocol.
proto-up	(Optional) Modifies the interface and protocol status to up even if the router is not connected to a wire or the interface of the peer router is down.

Command Default

The time interval between messages is10 seconds, and the number of retries is 3.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
10.0	This command was introduced.
12.2(8)T	This command was modified. The *retries* argument was added and made available on tunnel interfaces.
12.2(13)T	This command was modified. The default value for the *retries* argument was increased to 5.
12.2SX	This command was added 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.
15.1(4)M8	This command was modified. The **proto-up** keyword was added.
15.2(2)SNI	This command was implemented on the Cisco ASR 901 Series Aggregation Services Routers.
15.3(1)S	This command was integrated into Cisco IOS Release15.3(1)S.

Usage Guidelines

The **service interval**command must be enabled to run the **no keepalive**command.

Defaults for the keepalive Command

If you enter only the keepalive command with no arguments, default values for both arguments are used. If you enter the keepalive command and the timeout parameter, the default number of retries (5) is used. If you enter the **nokeepalive**command, keepalive packets are disabled on the interface. When the interface goes down, the session continues without shutting down because the keepalive packets are disabled.

Keepalive Time Interval

You can configure the keepalive time interval, which is the frequency at which the Cisco IOS software sends messages to itself (Ethernet and Token Ring) or to the other end (serial and tunnel), to ensure that a network interface is alive. The interval is adjustable in 1-second increments down to 1 second. An interface is declared down after five update intervals have passed without receiving a keepalive packet unless the retry value is set higher. If you are running a Cisco IOS image prior to Cisco IOS Release 12.2(13)T, the default retry value is 3.



Note Ethernet interface drivers on some access platforms use the keepalive time as the interval to test for network connectivity. By default, Ethernet link failure detection occurs between 1 and 9 seconds. Keepalive packets are still transmitted on the interface during this time.

Setting the keepalive timer to a low value is very useful for rapidly detecting Ethernet interface failures (transceiver cable disconnecting, cable not terminated, and so on).

Line Failure

A typical serial line failure involves losing the Carrier Detect (CD) signal. Because this sort of failure is typically noticed within a few milliseconds, adjusting the keepalive timer for quicker routing recovery is generally not useful.

Keepalive Packets with Tunnel Interfaces

Generic routing encapsulation (GRE) keepalive packets may be sent from both sides of a tunnel or from just one side. If they are sent from both sides, the period and retry parameters can be different at each side of the link. If you configure keepalives on only one side of the tunnel, the tunnel interface on the sending side might perceive the tunnel interface on the receiving side to be down because the sending interface is not receiving keepalives. From the receiving side of the tunnel, the link appears normal because no keepalives were enabled on the second side of the link.

Dropped Packets

Keepalive packets are treated as ordinary packets, so it is possible that they will be dropped. To reduce the chance that dropped keepalive packets will cause the tunnel interface to be taken down, increase the number of retries.



Note When adjusting the keepalive timer for a very low bandwidth serial interface, large datagrams can delay the smaller keepalive packets long enough to cause the line protocol to go down. You may need to experiment to determine the best values to use for the timeout and the number of retry attempts.

GRE Tunnels with IPsec

When GRE is used with IPsec, the keepalives are encrypted like any other traffic. As with user data packets, if the IKE and IPsec security associations are not already active on the GRE tunnel, the first GRE keepalive packet will trigger IKE/IPsec initialization.



Note GRE tunnel with IPSEC tunnel protection does not encrypt replies to incoming GRE keepalive packets. For more information, see the GRE Tunnel Keepalive Troubleshooting Technical Notes.

Examples

The following example shows how to enable keepalive packets and set the keepalive interval to 3 seconds:

```
Router(config)# interface ethernet 0
Router(config-if)# keepalive 3
```

The following example shows how to enable keepalive packets, set the keepalive interval to 3 seconds, and the retry value to 7 in a tunnel interface:

```
Router(config)# interface tunnel 1
Router(config-if)# keepalive 3 7
```

The following example shows how to bring up the interface of a router even if the peer router is down.

```
Router(config)# interface tunnel 1
Router(config)# service internal
Router(config-if)# no keepalive proto-up
```

Related Commands

Command	Description
service internal	Sets a primary or secondary IP address for an interface.