

F through H

- fabric buffer-reserve, on page 4
- fabric clear-block, on page 6
- fabric error-recovery fabric-switchover (virtual switch), on page 7
- fabric lcd-banner, on page 8
- fabric required, on page 10
- fabric switching-mode allow, on page 12
- fabric switching-mode force bus-mode, on page 15
- fabric timer, on page 17
- facility-alarm, on page 18
- facility-alarm critical exceed-action shutdown, on page 20
- facility-alarm detect, on page 21
- factory-reset all, on page 23
- factory-reset keep-licensing-info, on page 24
- factory-reset all secure 3-pass, on page 25
- fddi burst-count, on page 26
- fddi c-min, on page 27
- fddi cmt-signal-bits, on page 28
- fddi duplicate-address-check, on page 30
- fddi encapsulate, on page 31
- fddi frames-per-token, on page 33
- fddi smt-frames, on page 34
- fddi tb-min, on page 35
- fddi tl-min-time, on page 36
- fddi token-rotation-time, on page 37
- fddi t-out, on page 38
- fddi valid-transmission-time, on page 39
- fdl, on page 40
- flowcontrol, on page 42
- frame-relay, on page 44
- framing, on page 46
- framing (CEM), on page 48
- framing (E3 controller), on page 50
- framing (SONET), on page 52

- framing (T1 E1 controller), on page 53
- framing (T3 controller), on page 55
- framing (T3-E3 interface), on page 57
- full-duplex, on page 59
- g709 disable, on page 62
- g709 fec, on page 63
- g709 odu report, on page 64
- g709 odu overhead tti, on page 66
- g709 odu threshold, on page 67
- g709 otu report, on page 69
- g709 otu threshold, on page 71
- g709 tti-processing enable, on page 73
- gnss, on page 74
- gtp, on page 75
- half-duplex, on page 77
- half-duplex controlled-carrier, on page 79
- half-duplex timer, on page 81
- history (interface), on page 83
- hold-queue, on page 86
- hssi external-loop-request, on page 89
- hssi internal-clock, on page 90
- hub, on page 91
- hw-module boot, on page 92
- hw-module energywise level, on page 94
- hw-module fan-tray version, on page 96
- hw-module interface als restart, on page 98
- hw-module main-cpu qa error-recovery, on page 99
- hw-module mode, on page 101
- hw-module oversubscription, on page 103
- hw-module power-supply power-cycle, on page 104
- hw-module pxf stall-monitoring, on page 105
- hw-module reset, on page 106
- hw-module sec-cpu reset, on page 107
- hw-module shutdown, on page 109
- hw-module simulate link-up, on page 110
- hw-module slot, on page 111
- hw-module slot (6500), on page 114
- hw-module slot (7300), on page 117
- hw-module slot (7600), on page 119
- hw-module slot (ASR 1000 Series), on page 122
- hw-module slot image, on page 125
- hw-module slot subslot only, on page 126
- hw-module standby, on page 128
- hw-module subslot, on page 130
- hw-module subslot (4400), on page 132
- hw-module subslot ethernet vlan unlimited, on page 134

- hw-module subslot (LAN WAN), on page 136
- hw-module subslot service-engine session, on page 138
- hw-module subslot session, on page 140
- hw-module subslot shutdown, on page 141
- hw-module subslot shutdown (4400), on page 143

fabric buffer-reserve

To reserve ASIC buffers, use the **fabricbuffer-reserve** command. in global configuration mode. To return to the default settings, use the **no** form of this command.

fabric buffer-reserve [**high** | **low** | **medium***value*]
[**default**] **fabric buffer-reserve queue**
no fabric buffer-reserve

Syntax Description

high	(Optional) Reserves the high (0x5050) ASIC buffer spaces.
low	(Optional) Reserves the low (0x3030) ASIC buffer spaces.
medium	(Optional) Reserves the medium (0x4040) ASIC buffer spaces.
value	(Optional) 16-bit value; valid values are from 0x0 to 0x5050.
default	(Optional) Specifies the default queue setting.
queue	Specifies the queue setting for the buffer reserve.

Command Default

The default settings are as follows:

- Buffer reserve is set to 0x0.
- Two queues.

Command Modes

Global configuration

Command History

Release	Modification
12.2(18)SXE	Support for this command was introduced on the Supervisor Engine 720.
12.2(18)SXF	This command was changed to add the **queue** keyword.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

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

This command is not supported on Cisco 7600 series routers that are configured with a Supervisor Engine 32.

The **fabricbuffer-reservequeue**command is supported on Cisco 7600 series routers that are configured with the following modules:

- WS-X6748-GE-TX
- WS-X6724-SFP

- WS-X6748-SFP
- WS-X6704-10GE

Entering the **defaultfabricbuffer-reservequeue** command is the same as entering the **fabricbuffer-reservequeue** command.

You can enter the **fabricbuffer-reserve** command to improve the system throughput by reserving ASIC buffers.

This command is supported on the following modules:

- WS-X6704-10GE
- WS-X6748-SFP
- WS-X6748-GE-TX
- WS-X6724-SFP

Examples

This example shows how to reserve the high (0x5050) ASIC buffer spaces:

```
Router(config)# fabric buffer-reserve high
Router(config)#
```

This example shows how to reserve the low (0x3030) ASIC buffer spaces:

```
Router(config)# fabric buffer-reserve low
Router(config)#
```

fabric clear-block

To enable the clear-block congestion control for the fabric channels, use the **fabricclear-block** command in global configuration mode. To disable the clear-block congestion control for the fabric channels, use the **no** form of this command.

fabric clear-block
no fabric clear-block

Syntax Description

This command has no arguments or keywords.

Command Default

Disabled

Command Modes

Global configuration

Command History

Release	Modification
12.2(17d)SXB1	Support for this command was introduced on the Supervisor Engine 720.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

Note Do not enter the **fabricclear-block**command unless TAC advises you to do so.

This command is supported only with Supervisor Engine 720 hardware revision 4.0 and later releases.

This command is not supported on Cisco 7600 series routers that are configured with a Supervisor Engine 32.

Examples

This example shows how to enable the clear-block congestion control for the fabric channels:

```
Router(config)# fabric clear-block
Router(config)#
```

This example shows how to disable the clear-block congestion control for the fabric channels:

```
Router(config)# no fabric clear-block
Router(config)#
```

fabric error-recovery fabric-switchover (virtual switch)

To enable a supervisor engine switchover when excessive fabric synchronization errors are detected on the fabric-enabled module, use the **fabricerror-recoveryfabric-switchover** command in global configuration mode. To disable the supervisor engine switchover for excessive fabric synchronization errors, use the **no** form of this command.

fabric switch *num* **error-recovery fabric-switchover**
no fabric switch *num* **error-recovery fabric-switchover**

Syntax Description

switch *num*	Specifies the switch number; valid values are 1 and 2.

Command Default

Excessive fabric synchronization errors initiate a supervisor engine switchover, and the configuration is not saved to the configuration file.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(33)SXH1	Support for this command was introduced.

Usage Guidelines

When a fabric-capable switching module has fabric errors, a supervisor engine switchover is initiated.

You can use the **nofabricerror-recoveryfabric-switchover** command to avoid the supervisor engine switchover. This command does not perform the supervisor engine switchover but powers down the module that is experiencing the excessive fabric errors. This command is saved to the configuration file.

Examples

The following example shows how to enable a supervisor engine switchover when excessive fabric synchronization errors are detected on the fabric-enabled module:

```
Router(config)# fabric switch 2 error-recovery fabric-switchover
Router(config)#
```

The following example shows how to disable a supervisor engine switchover when excessive fabric synchronization errors are detected on the fabric-enabled module:

```
Router(config)# no fabric switch 2 error-recovery fabric-switchover
Router(config)#
```

Related Commands

Command	Description
show fabric	Displays the information about the crossbar fabric .

fabric lcd-banner

To specify the message-of-the-day (MOTD) banner for display on the Switch Fabric Module, use the **fabriclcd-banner** command in global configuration mode. To delete the MOTD banner, use the **no** form of this command.

fabric lcd-banner *d message d*
no fabric lcd-banner

Syntax Description

d	Delimiting character; see the "Usage Guidelines" section for additional guidelines.
message	Message text; see the "Usage Guidelines" section for additional guidelines.

Command Default

No MOTD banner is specified.

Command Modes

Global configuration

Command History

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

Usage Guidelines

This command is supported on Cisco 7600 series routers that are configured with a Supervisor Engine 2 only.

This command is not supported on Cisco 7600 series routers that are configured with a Supervisor Engine 32

You cannot use the delimiting character in the banner message. The delimiter is a character of your choice--a pound sign (#), for example.

You can replace tokens with the corresponding configuration argument.

Follow this command with one or more blank spaces and a delimiting character of your choice. Then enter one or more lines of text, terminating the message with the second occurrence of the delimiting character.

This MOTD banner is useful for displaying messages that affect all users (such as impending system shutdowns).

When you connect to the router, the MOTD banner appears before the login prompt. After you successfully log in to the router, the EXEC banner or incoming banner is displayed, depending on the type of connection. For a reverse Telnet login, the incoming banner is displayed. For all other connections, the router displays the EXEC banner.

To customize the banner, use tokens in the form $(token) in the message text. Tokens display current Cisco IOS configuration arguments, such as the router's hostname and IP address.

The table below describes the command tokens.

Table 1: Command Tokens

Token	Information Displayed in the Banner
$(hostname)	Displays the router's hostname.

$(domain)	Displays the router's domain name.
$(line)	Displays the VTY or TTY (async) line number.
$(line-desc)	Displays the description that is attached to the line.

Examples

This example shows how to set a MOTD banner for display on the Switch Fabric Module LCD display; the pound sign (#) is used as a delimiting character:

```
Router(config)# fabric lcd-banner#
Building power will be off from 7:00 AM until 9:00 AM this coming Tuesday.
#
```

This example shows how to set a MOTD banner; the percent sign (%) is used as a delimiting character:

```
Router(config)# fabric lcd-banner%
Enter TEXT message.  End with the character '%'.
You have entered $(hostname).$(domain) on line $(line) ($(line-desc)) %
```

When the MOTD banner is executed, you see the following (notice that the $(token) syntax is replaced by the corresponding configuration argument):

```
You have entered company.ourdomain.com on line 5 (Dialin Modem)
```

Related Commands

Command	Description
banner exec	Specifies and enables a message to be displayed when an EXEC process is created.
banner incoming	Defines and enables a banner to be displayed when there is an incoming connection to a terminal line from a host on the network.
banner login	Defines and enables a customized banner to be displayed before the username and password login prompts.
banner slip-ppp	Allows customization of the banner that is displayed when a SLIP or PPP connection is made.
exec-banner	Reenables the display of EXEC and MOTD banners on the specified line or lines.
motd-banner	Enables the display of MOTD banners on the specified line or lines.

fabric required

To prevent the Cisco 7600 series routers from coming online without a Switch Fabric Module, use the **fabricrequired**command in global configuration mode. To allow the Cisco 7600 series routers to come up without a Switch Fabric Module, use the **no** form of this command.

fabric required
no fabric required

Syntax Description

This command has no arguments or keywords.

Command Default

A Switch Fabric Module is not required.

Command Modes

Global configuration

Command History

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

Usage Guidelines

This command is not supported on Cisco 7600 series routers that are configured with a Supervisor Engine 32.

If you enter the **fabricrequired** command, when you remove or power down the last Switch Fabric Module, all modules except the supervisor engine, power down. When you insert or power on the first Switch Fabric Module, the modules that were previously powered down power up if the Switch Fabric Module configuration is not in conflict with other configurations.

If you enter the **nofabricrequired** command, the modules will also power on if a Switch Fabric Module is not present and the configuration allows for it.

Examples

This example shows how to prevent the Cisco 7600 series routers from coming online without a Switch Fabric Module:

```
Router(config)#
fabric required
Router(config)#
```

This example shows how to allow the Cisco 7600 series routers to come up without a Switch Fabric Module:

```
Router(config)#
no fabric required
Router(config)#
```

Related Commands

Command	Description
show fabric	Displays the information about the crossbar fabric.

fabric switching-mode allow

To enable various switching modes in the presence of two or more fabric-enabled switching modules, use the **fabricswitching-modeallow** command in global configuration mode. To disable the settings, use the **no** form of this command.

fabric switching-mode allow {**bus-mode** | **dcef-only** | **truncated** [**threshold** [*mod*]]}
no fabric switching-mode allow {**bus-mode** | **truncated** [**threshold**]}

Syntax Description

bus-mode	Specifies a module to run in bus mode.
dcef-only	Allows switching in distributed Cisco Express Forwarding (dCEF)-only mode.
truncated	Specifies a module to run in truncated mode.
threshold *mod*	(Optional) Specifies the number of fabric-enabled modules for truncated switching mode; see the "Usage Guidelines" section for additional information.

Command Default

The truncated mode is disabled.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(14)SX	This command was introduced on the Supervisor Engine 720.
12.2(17d)SXB	This command was modified. This command supports the Supervisor Engine 2.
12.2(18)SXD1	This command was modified. The **dcef-only** keyword was added on the Supervisor Engine 2.
12.2(18)SXE	This command was modified. Support for OIR performance enhancement and the **dcef-only** keyword was added on the Supervisor Engine 720.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was modified. This command was introduced on the Supervisor Engine 720-10GE.

Usage Guidelines

This command is not supported on Catalyst 6500 or Cisco 7600 series routers that are configured with a Supervisor Engine 32.

Ethernet ports are not disabled when this command is entered on a Supervisor Engine 720-10GE. This command is also supported with Supervisor Engine 720 starting with Release 12.2(33)SXI2. However, prior to Release 12.2(33)SXI2, if all the installed switching modules have Distributed Forwarding Cards (DFCs), enter the **fabricswitching-modeallowdcef-only** command to disable the Ethernet ports on both supervisor engines. Entering this command ensures that all modules are operating in dCEF-only mode and simplifies switchover to the redundant supervisor engine.

With a Supervisor Engine 2 and Release 12.2(18)SXD1 and later releases, if all the installed switching modules have DFCs, enter the **fabricswitching-modeallowdcef-only** command to disable the Ethernet ports on the

redundant supervisor engine. Entering this command ensures that all modules are operating in dCEF-only mode.

Note The **fabricswitching-modeallowdcef-only** command is accepted only in stateful switchover (SSO) redundancy mode.

Bus mode--Supervisor engines use this mode for traffic between nonfabric-enabled modules and for traffic between a nonfabric-enabled module and a fabric-enabled module. In this mode, all traffic passes between the local bus and the supervisor engine bus.

dCEF-only--Supervisor engines, both active and redundant, operate as nonfabric-capable modules with their uplink ports relying on the Policy Feature Card (PFC) on the active supervisor engine for all forwarding decisions. For the Supervisor 720-10G, the uplink ports on both the active and standby routers will remain active. If all other modules are operating in dCEF-only mode, module Online Insertion and Removal (OIR) is nondisruptive.

Note The system message "PSTBY-2-CHUNKPARTIAL: Attempted to destroy partially full chunk, chunk 0xB263638, chunk name: MET FREE POOL" is displayed on the Supervisor Engine if both the **fabricswitching-modeallowdcef-only** and **ipv6mfibhardware-switchinguplink** commands are configured. The router will ignore the command configured last.

Truncated mode--Supervisor engines use this mode for traffic between fabric-enabled modules when there are both fabric-enabled and nonfabric-enabled modules installed. In this mode, line cards send a truncated version of the traffic (the first 64 bytes of the frame) over the Catalyst bus.

Compact mode--Supervisor engines use this mode for all traffic when only fabric-enabled modules are installed. In this mode, a compact version of the Desktop Bus (DBus) header is forwarded over the Catalyst bus, which provides the best possible centralized forwarding performance.

A fabric-enabled module has an additional connection directly to the switch fabric. Fabric-enabled modules forward packets in compressed mode, where only the header is sent to the Supervisor Engine and the full packet is forwarded directly from one line card to another.

To prevent use of nonfabric-enabled modules or to prevent fabric-enabled modules from using bus mode, enter the **nofabricswitching-modeallowbus-mode** command.

Caution Entering the **nofabricswitching-modeallowbus-mode** command removes power from any nonfabric-enabled modules that are installed.

The **fabricswitching-modeallow** c ommand affects Supervisor engines that are configured with a minimum of two fabric-enabled modules.

You can enter the **fabricswitching-modeallowtruncated** command to unconditionally allow truncated mode.

You can enter the **nofabricswitching-modeallowtruncated** command to allow truncated mode if the threshold is met.

You can enter the **nofabricswitching-modeallowbus-mode**command to prevent any module from running in bus mode.

To return to the default truncated-mode threshold, enter the **nofabricswitching-modeallowtruncatedthreshold** command.

The valid value for *mod*is the threshold value.

Examples

The following example shows how to specify truncated mode:

```
Router(config)#
fabric switching-mode allow truncated
```

Related Commands

Command	Description
ipv6 mfib hardware-switching uplink	Configures MFIB hardware switching for IPv6 multicast packets on a global basis.
show fabric	Displays the information about the crossbar fabric.

fabric switching-mode force bus-mode

To force fabric-enabled modules into bus switching mode, use the**fabricswitching-modeforcebus-mode** command in global configuration mode. To power cycle the module to truncated mode, use the **no** form of this command.

fabric switching-mode force bus-mode
no fabric switching-mode force bus-mode

Syntax Description

This command has no arguments or keywords.

Command Default

This command has no default settings.

Command Modes

Global configuration

Command History

Release	Modification
12.2(18)SXD5	Support for this command was introduced on the Supervisor Engine 720.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

This command is not supported on Cisco 7600 series routers that are configured with a Supervisor Engine 32.

This command applies to the following modules:

- WS-SVC-FWM-1-K9--Firewall Services Module
- WS-SVC-IDS2-BUN-K9--Intrusion Detection Service Module 2
- WS-SVC-MWAM-1--Multiprocessor WAN Application Module
- WS-SVC-NAM-1--Network Analysis Module 1
- WS-SVC-NAM-2--Network Analysis Module 2
- WS-SVC-PSD-1--Persistent Storage Device Module
- WS-SVC-SSL-1-K9--SSL Module
- WS-SVC-WLAN-1-K9--Wireless LAN Service Module

After you enter the **fabricswitching-modeforcebusmode** or the **nofabricswitching-modeforcebusmode**command, the fabric-enabled service modules power cycle immediately. The mode change occurs as the modules come up after the power cycle.

Examples

This example shows how to force fabric-enabled modules into flow-through switching mode:

```
Router(config)#
fabric switching-mode force bus-mode
Router(config)#
```

Related Commands

Command	Description
show fabric	Displays the information about the crossbar fabric.

fabric timer

To set the drop counter time-stamp and peak-utilization poll time in seconds, use the **fabrictimer**command in global configuration mode. To remove the drop counter time-stamp and peak-utilization poll time, use the **no** form of this command.

fabric timer *seconds*
no fabric timer *seconds*

Syntax Description

seconds	Poll time in seconds for drop counter time-stamps and peak-utilization. Valid values are from 1 to 1800.

Command Default

The internal default timer is set to 15 seconds.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(14)SXF	This command was introduced on the Catalyst 6500 series switch.
12.2(5)SRB	This command was implemented on the Supervisor Engine 720.

Examples

The following example shows how to set the drop counter time-stamp and peak-utilization poll time to 200 seconds:

```
Router(config)#
fabric timer 200
```

Related Commands

Command	Description
show fabric	Displays the information about the crossbar fabric.

facility-alarm

To configure threshold temperatures for minor, major, and critical alarms, use the **facility-alarm** command in global configuration mode. To disable alarms for the threshold and reset the threshold to the default value, use the no form of this command.

Cisco 10000 Series Router
facility-alarm {**core-temperature** | **outlet-temperature**} {**major** | **minor** | **critical**} [*temperature*]
no facility-alarm {**core-temperature** | **outlet-temperature**} {**major** | **minor** | **critical**} [*temperature*]

Cisco 7200 Series Router
facility-alarm {**core-temperature** | **intake-temperature**} *temperature*

Syntax Description

core-temperature	Specifies that the alarm applies to the temperature of the internal core of the router. The temperature sensor close to the router's processor measures the core temperature.
outlet-temperature	Specifies that the alarm applies to the air flow temperature. **Note** This keyword is valid only on the Cisco 10000 series router for the PRE3.
major [*temperature*	Specifies the alarm threshold temperature threshold in degrees C. The default value is 53 degrees C. Major alarms affect several subscribers that connect to the reporting node.
minor [*temperature*	Specifies the alarm threshold temperature threshold in degrees C. The default value is 45 degrees C. Minor alarms affect a single or small number of subscribers who connect to the reporting node.
critical [*temperature*	Specifies the alarm threshold temperature threshold in degrees C. The default value is 85 Celsius C. Critical alarms affect most or all subscribers that connect to the reporting node.
temperature	Temperature threshold in degrees C. The range is 30 to 70 degrees C.

Command Default

If the command is not enabled, the default values are set.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.0(17)SL	This command was introduced on the Cisco 10000 series router.
12.2(16)BX	This command was introduced on the PRE2.
12.2(31)SB2	This command was introduced on the PRE3 for the Cisco 10000 series router.

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

Usage Guidelines

You can configure explicit threshold temperatures to override the defaults for major, minor, and critical alarms. Temperature thresholds for each alarm type and location are automatically set based on determined values that vary depending on the number and type of boards inserted in the chassis. In addition to the automatically set thresholds, you can set thresholds for minor and major temperature alarms. You can also disable the minor and major temperature alarms. You cannot, however, change the threshold for or disable critical alarms.

Cisco 10000 Series Router

On the PRE2, use the **facility-alarmcore-temperature** command. On the PRE3, use the **facility-alarmoutlet-temperature** command.

The default value for a threshold temperature depends on the performance routing engine (PRE) installed in the router as the following describes:

- Major alarm
  - PRE2--The default value is 53.
  - PRE3--The default value is 58.
- Minor alarm
  - PRE2--The default value is 45.
  - PRE3--The default value is 50.
- Critical alarm
  - PRE2--The default value is 85.
  - PRE3--The default value is 85.

Examples

The following example sets a threshold temperature of 53 for major alarms on the PRE2:

```
Router> enable
Router# config terminal
Router(config)# facility-alarm core-temperature major 53
```

The following example sets a threshold temperature of 50 for minor alarms on the PRE3:

```
Router> enable
Router# config terminal
Router(config)# facility-alarm core-temperature minor 50
```

Related Commands

Command	Description
clear facility-alarm	Clears alarm conditions and resets the alarm contacts.
show facility-alarm status	Displays the current major, minor, and critical alarm status, if any, and displays the configuration of the alarm thresholds.

facility-alarm critical exceed-action shutdown

To allow automatic router shutdown, use the facility-alarm critical exceed-action shutdown command in global configuration mode. To disable automatic router shutdown, use the **no** form of this command.

facility-alarm critical exceed-action shutdown
no facility-alarm critical exceed-action shutdown

Syntax Description

This command has no arguments or keywords.

Command Default

Automatic router shutdown is not enabled.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Release 2.1	This command was introduced on the Cisco ASR 1000 Series Routers.

Usage Guidelines

If the facility-alarm critical exceed-action shutdown command is enabled, the router performs an automatic shutdown under the following conditions:

- The internal temperature of the router or a power supply exceeds the temperature threshold.
- The voltage of an AC or DC power supply is out of tolerance.

Examples

The following example enables automatic router shutdown:

```
Router(config)# facility-alarm critical exceed-action shutdown
```

Related Commands

Command	Description
show facility-alarm	Displays the status of a generated alarm.

facility-alarm detect

To turn on the facility alarms, use the **facility-alarmdetect** command in global configuration mode. To turn off the alarm, use the **no** form of this command.

facility-alarm detect {**controller** *controller slot-number* | **interface** *type number* | **rps** | **temperature** | **fan**}
no facility-alarm detect {**controller T1** *slot-number* | **interface** *type number* | **rps** | **temperature** | **fan**}

Syntax Description

controller	Specifies the facility alarm for controllers.
controller slot-number	Specifies the controller. The controller can be one of the following: • **E1** --The range of the slot value is from 1 to 7 and the range of the port is from 0 to 7. • **T1** --The range of the slot value is from 1 to 7 and the range of the port is from 0 to 7. • **T3** --The range of the slot value is from 1 to 7.
interface	Specifies the facility alarm for interfaces.
type	Interface type. For more information, use the question mark (?) online help function.
number	Interface or subinterface number. For more information about the numbering syntax for your networking device, use the question mark (?) online help function.
rps	Specifies the facility alarm for the redundant power supply (RPS).
temperature	Specifies the facility alarm for the environmental monitor temperature.
fan	Specifies the facility alarm for the environmental monitor fans.

Command Default

The facility alarm is turned off.

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 on the Cisco 5400-XM series routers.

Usage Guidelines

Facility alarms monitor the following failure events:

- CT1/CE1/CT3 controller down
- Interface down
- RPS failure

- Trunk card failure

Cisco IOS software polls every second to detect the failure events that you have configured and turns on the alarm when any one of the failure events is detected. By default, the facility alarm is off. Users have to configure a facility alarm command to enable monitoring of the failure conditions.

Examples

The following example shows how to turn on the facility alarm for RPS:

```
Router(config)# facility-alarm detect rps
```

Related Commands

Command	Description
show facility-alarm	Displays the status of a generated alarm.

factory-reset all

To erase all the user-configured data, use the **factory-reset all** command in EXEC mode:

factory-reset all

Syntax Description

Syntax Description

This command has no keywords or arguments.

Command Modes

EXEC mode

Command History

Release	Modification
Cisco IOS XE Bengaluru Release 17.6.1	This command was introduced on ASR 900, ASR 920, and NCS 4200 platforms.

Usage Guidelines

The command erases the following data:

- All writable file systems and personal data
- OBFL logs
- User data and startup configuration
- ROMMON variables
- User credentials
- License information

Examples

The following example shows the configuration of the command:

```
Router>enable
Router>factory-reset all
```

factory-reset keep-licensing-info

To erase all the user-configured data except the licensing information, use the **factory-reset keep-licensing-info** command in EXEC mode:

factory-reset keep-licensing-info

Syntax Description

Syntax Description

This command has no keywords or arguments.

Command Modes

EXEC mode

Command History

Release	Modification
Cisco IOS XE Bengaluru Release 17.6.1	This command was introduced on ASR 900, ASR 920, and NCS 4200 platforms.

Usage Guidelines

This command erases the following user-configured data:

- All writable file systems and personal data
- OBFL logs
- User data and startup configuration
- ROMMON variables
- User credentials

Examples

The following example shows the configuration of the command:

```
enable
factory-reset keep-licensing-info
```

factory-reset all secure 3-pass

To erase all data using the the National Industrial Security Program Operating Manual (DoD 5220.22-M) Wiping Standard, use the **factory-reset all secure 3-pass-DoD 5220-22-M** command in EXEC mode:

factory-reset all-secure 3-pass-DoD 5220-22-M

Syntax Description

Syntax Description

This command has no keywords or arguments.

Command Modes

EXEC mode

Command History

Release	Modification
Cisco IOS XE Bengaluru Release 17.6.1	This command was introduced on ASR 900, ASR 920, and NCS 4200 platforms.

Usage Guidelines

The commands erases the following data

- All writable file systems and personal data using the the National Industrial Security Program Operating Manual (DoD 5220.22-M) Wiping Standard:
- OBFL logs
- User data and startup configuration
- ROMMON variables
- User credentials
- License information

Examples

The following example shows the configuration of the command:

```
enable
factory-reset all-secure 3-pass
DoD 5220-22-M
```

fddi burst-count

To allow the FCI card to preallocate buffers to handle bursty FDDI traffic (for example, Network File System [NFS] bursty traffic), use the **fddiburst-count** command in interface configuration mode. To revert to the default value, use the **no** form of this command.

fddi burst-count *number*
no fddi burst-count

Syntax Description

number	Number of preallocated buffers in the range from 1 to 10. The default is 3.

Command Default

3 buffers

Command Modes

Interface configuration

Command History

Release	Modification
10.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

This command applies to the FCI card only.

Note The microcode software version should *not* be 128.45 or 128.43.

Examples

The following example sets the number of buffers to 5:

```
Router(config)# interface fddi 0
Router(config-if)# fddi burst-count 5
```

fddi c-min

To set the C-Min timer on the pulse code modulation (PCM), use the **fddic-min** command in interface configuration mode. To revert to the default value, use the **no** form of this command.

fddi c-min *microseconds*
no fddi c-min

Syntax Description

microseconds	Sets the timer value, in microseconds. The default is 1600.

Command Default

1600 microseconds

Command Modes

Interface configuration

Command History

Release	Modification
10.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

This command applies to the processor connection management (CMT) only. You need extensive knowledge of the PCM state machine to tune this timer. Use this command when you run into PCM interoperability problems.

Examples

The following example sets the C-Min timer to 2000 microseconds:

```
Router(config)# interface fddi 0
Router(config-if)# fddi c-min 2000
```

Related Commands

Command	Description
fddi tb-min	Sets the TB-Min timer in the PCM.
fddi tl-min-time	Controls the TL-Min time (the minimum time to transmit a PHY line state before advancing to the PCM state, as defined by the X3T9.5 specification).
fddi t-out	Sets the t-out timer in the PCM.

fddi cmt-signal-bits

To control the information transmitted during the connection management (CMT) signaling phase, use the **fddicmt-signal-bits**command in interface configuration mode.

fddi cmt-signal-bits *signal-bits* [**phy-a** | **phy-b**]

Syntax Description

signal-bits	A hexadecimal number preceded by 0x; for example, 0x208. The FDDI standard defines 10 bits of signaling information that must be transmitted, as follows: • bit 0--Escape bit. Reserved for future assignment by the FDDI standards committee. • bits 1 and 2--Physical type, as defined in the first table below. • bit 3--Physical compatibility. Set if topology rules include the connection of a physical-to-physical type at the end of the connection. • bits 4 and 5--Link confidence test duration; set as defined in the second table below. • bit 6--MAC available for link confidence test. • bit 7--Link confidence test failed. The setting of bit 7 indicates that the link confidence was failed by the Cisco end of the connection. • bit 8--MAC for local loop. • bit 9--MAC on physical output.
phy-a	(Optional) Selects Physical Sublayer A. The default is 0x008 (hexadecimal) or 00 0000 1000 (binary). Bits 1 and 2 are set to 00 to select Physical A. Bit 3 is set to 1 to indicate “accept any connection.”
phy-b	(Optional) Selects Physical Sublayer B. The default is 0x20c (hexadecimal) or 10 0000 1100 (binary). Bits 1 and 2 are set to 10 to select Physical B. Bit 3 is set to 1 to indicate “accept any connection.” Bit 9 is set to 1 to select MAC on output. The normal data flow on FDDI is input on Physical A and output on Physical B.

Command Default

- **phy-a** is set to 0x008 (hexadecimal) or 00 0000 1000 (binary). Bits 1 and 2 are set to 00 to select Physical A. Bit 3 is set to 1 to indicate “accept any connection.”
- **phy-b** is set to 0x20c (hexadecimal) or 10 0000 1100 (binary). Bits 1 and 2 are set to 10 to select Physical B. Bit 3 is set to 1 to indicate “accept any connection.” Bit 9 is set to 1 to select MAC on output. The normal data flow on FDDI is input on Physical A and output on Physical B.

Command Modes

Interface configuration

Command History

Release	Modification
10.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

If neither the **phy-a** nor **phy-b** keyword is specified, the signal bits apply to both physical connections.

Caution Use of the **fddicmt-signal-bits** configuration command is *not* recommended under normal operations. This command is used when debugging specific CMT implementation issues.

The table below lists the physical types.

Table 2: FDDI Physical Type Bit Specifications

Bit 2	Bit 1	Physical Type
0	0	Physical A
1	0	Physical B
0	1	Physical S
1	1	Physical M

The table below lists the duration bits.

Table 3: FDDI Link Confidence Test Duration Bit Specification

Bit 5	Bit 4	Test Duration
0	0	Short test (default 50 milliseconds)
1	0	Medium test (default 500 milliseconds)
0	1	Long test (default 5 seconds)
1	1	Extended test (default 50 seconds)

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

Examples

The following example sets the CMT signaling phase to signal bits 0x208 on both physical connections:

```
Router(config)# interface fddi 0
Router(config-if)# fddi cmt-signal-bits 0x208
```

fddi duplicate-address-check

To enable the duplicate address detection capability on the FDDI interface, use the **fddiduplicate-address-check** command in interface configuration mode. To disable this function, use the **no** form of this command.

fddi duplicate-address-check
no fddi duplicate-address-check

Syntax Description

This command has no arguments or keywords.

Command Default

Disabled

Command Modes

Interface configuration

Command History

Release	Modification
10.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

If you use this command, the Cisco IOS software will detect a duplicate address if multiple stations are sharing the same MAC address. If the software finds a duplicate address, it will shut down the interface.

Examples

The following example enables duplicate address checking on the FDDI interface:

```
Router(config)# interface fddi 0
Router(config-if)# fddi duplicate-address-check
```

fddi encapsulate

To specify encapsulating bridge mode on the CSC-C2/FCIT interface card, use the **fddiencapsulate** command in interface configuration mode. To turn off encapsulation bridging and return the FCIT interface to its translational, nonencapsulating mode, use the **no**form of this command.

fddi encapsulate
no fddi encapsulate

Syntax Description

This command has no arguments or keywords.

Command Default

By default, the FDDI interface uses the SNAP encapsulation format defined in RFC 1042, *Standard for the Transmission of IP Datagrams Over IEEE 802 Networks* . It is not necessary to define an encapsulation method for this interface when using the CSC-FCI interface card.

Command Modes

Interface configuration

Command History

Release	Modification
10.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

The **nofddiencapsulate** command applies only to CSC-C2/FCIT interfaces, because the CSC-FCI interfaces are always in encapsulating bridge mode. The CSC-C2/FCIT interface card fully supports transparent and translational bridging for the following configurations:

- FDDI to FDDI
- FDDI to Ethernet
- FDDI to Token Ring

The **fddiencapsulate** command puts the CSC-C2/FCIT interface into encapsulation mode when doing bridging. In transparent mode, the FCIT interface interoperates with earlier versions of the CSC-FCI encapsulating interfaces when performing bridging functions on the same ring.

Caution Bridging between dissimilar media presents several problems that can prevent communications from occurring. These problems include bit-order translation (or usage of MAC addresses as data), maximum transfer unit (MTU) differences, frame status differences, and multicast address usage. Some or all of these problems might be present in a multimedia bridged LAN and might prevent communication from taking place. These problems are most prevalent when bridging between Token Rings and Ethernets or between Token Rings and FDDI nets. This is because of the different way Token Ring is implemented by the end nodes.

The following protocols have problems when bridged between Token Ring and other media: Novell IPX, DECnet Phase IV, AppleTalk, VINES, XNS, and IP. Furthermore, the following protocols may have problems when bridged between FDDI and other media: Novell IPX and XNS. We recommend that these protocols be routed whenever possible.

Examples

The following example sets FDDI interface 1 on the CSC-C2/FCIT interface card to encapsulating bridge mode:

```
Router(config)# interface fddi 1
Router(config-if)# fddi encapsulate
```

fddi frames-per-token

To specify the maximum number of frames that the FDDI interface transmits per token capture, use the **fddiframes-per-token** command in interface configuration mode. To revert to the default value, use the **no** form of this command.

fddi frames-per-token *number*
no fddi frames-per-token

Syntax Description

number	Maximum number of frames to transmit per token capture. Valid values are from 1 to 10. The default is 3.

Command Default

3 frames

Command Modes

Interface configuration

Command History

Release	Modification
11.2 P	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

Changing the value will increase or decrease the maximum number of frames that the FDDI interface can transmit when it receives a token. Increasing the value does not necessarily mean more frames will be transmitted on each token capture. This is heavily dependent on the traffic load of the specific interface.

When the interface captures a token, it transmits all of the frames that are queued in the interface's transmit ring, up to a maximum value specified by the**fddiframes-per-token** command.

If there are no frames ready for transmission, the token is passed on, and no frames are transmitted. If there are less than the **fddiframes-per-token**valuein the transmit ring, all frames in the transmit ring are transmitted before the token is passed on. If there are more than the **fddiframes-per-token**value in the transmit ring, the specified value is transmitted before the token is passed on. The remaining frames in the transmit ring remain queued until the token is captured again.

Examples

The following example shows how to configure the FDDI interface to transmit four frames per token capture:

```
Router(config-if)# fddi frames-per-token 4
```

fddi smt-frames

To enable the Station Management (SMT) frame processing capability on the FDDI, use the **fddismt-frames** command in interface configuration mode. To disable this function and prevent the Cisco IOS software from generating or responding to SMT frames, use the **no** form of this command.

fddi smt-frames
no fddi smt-frames

Syntax Description

This command has no arguments or keywords.

Command Default

Enabled

Command Modes

Interface configuration

Command History

Release	Modification
10.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

Use the **no** form of this command to turn off SMT frame processing for diagnosing purposes. Use the **fddismt-frames** command to reenable the feature.

Examples

The following example disables SMT frame processing:

```
Router(config)# interface fddi 0
Router(config-if)# no fddi smt-frames
```

fddi tb-min

To set the TB-Min timer in the physical connection management (PCM), use the **fdditb-min** command in interface configuration mode. To revert to the default value, use the **no** form of this command.

fddi tb-min *milliseconds*
no fddi tb-min

Syntax Description

milliseconds	Number, in milliseconds, that sets the TB-Min timer value. The range is from 0 to 65535. The default is 100.

Command Default

milliseconds : 100

Command Modes

Interface configuration

Command History

Release	Modification
10.3	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

This command applies to the processor connection management (CMT) only. Use this command when you run into PCM interoperability problems.

Note You need extensive knowledge of the PCM state machine to tune this timer.

Examples

The following example shows how to set the TB-Min timer to 200 ms:

```
Router(config)# interface fddi 0
Router(config-if)# fddi tb-min 200
```

Related Commands

Command	Description
fddi c-min	Sets the C-Min timer on the PCM.
fddi tl-min-time	Controls the TL-Min time (the minimum time to transmit a PHY line state before advancing to the PCM state, as defined by the X3T9.5 specification).
fddi t-out	Sets the t-out timer in the PCM.

fddi tl-min-time

To control the TL-Min time (the minimum time to transmit a Physical Sublayer, or PHY line state, before advancing to the next physical connection management [PCM] state, as defined by the X3T9.5 specification), use the **fdditl-min-time** command in interface configuration mode.

fddi tl-min-time *microseconds*

Syntax Description

microseconds	Number, in microseconds, that specifies the time used during the connection management (CMT) phase to ensure that signals are maintained for at least the value of TL-Min so that the remote station can acquire the signal. The range is from 0 to 4294967295. The default is 30.

Command Default

microseconds : 30

Command Modes

Interface configuration

Command History

Release	Modification
10.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

Interoperability tests have shown that some implementations of the FDDI standard need more than 30 microseconds to sense a signal.

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

Examples

The following example changes the TL-Min time from 30 microseconds to 100 microseconds:

```
Router(config)# interface fddi 0
Router(config-if)# fddi tl-min-time 100
```

The following example changes the TL-Min time from 30 microseconds to 100 microseconds on a Cisco 7500 series router:

```
Router(config)# interface fddi 3/0
Router(config-if)# fddi tl-min-time 100
```

Related Commands

Command	Description
fddi c-min	Sets the C-Min timer on the PCM.
fddi t-out	Sets the t-out timer in the PCM.

fddi token-rotation-time

To control ring scheduling during normal operation and to detect and recover from serious ring error situations, use the **fdditoken-rotation-time** command in interface configuration mode. To revert to the default value, use the **no** form of this command.

fddi token-rotation-time *microseconds*
no fddi token-rotation-time

Syntax Description

microseconds	Number, in microseconds, that specifies the token rotation time (TRT). The range is from 4000 to 165000. The default is 5000.

Command Default

microseconds : 5000

Command Modes

Interface configuration

Command History

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

Usage Guidelines

The FDDI standard restricts the allowed time to be greater than 4000 microseconds and less than 165,000 microseconds. As defined in the X3T9.5 specification, the value remaining in the TRT is loaded into the token holding timer (THT). Combining the values of these two timers provides the means to determine the amount of bandwidth available for subsequent transmissions.

Examples

The following example sets the rotation time to 24,000 microseconds:

```
Router(config)# interface fddi 0
Router(config-if)# fddi token-rotation-time 24000
```

The following example sets the rotation time to 24,000 microseconds on a Cisco 7500 series router:

```
Router(config)# interface fddi 3/0
Router(config-if)# fddi token-rotation-time 24000
```

fddi t-out

To set the timeout timer in the physical connection management (PCM), use the **fddit-out** command in interface configuration mode. To revert to the default value, use the **no** form of this command.

fddi t-out *milliseconds*
no fddi t-out

Syntax Description

milliseconds	Number, in milliseconds, that sets the timeout timer. The range is from 0 to 65535. The default is 100.

Command Default

milliseconds : 100

Command Modes

Interface configuration

Command History

Release	Modification
10.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

This command applies to the processor connection management (CMT) only. Use this command when you run into PCM interoperability problems.

Note You need extensive knowledge of the PCM state machine to tune this timer.

Examples

The following example sets the timeout timer to 200 ms:

```
Router(config)# interface fddi 0
Router(config-if)# fddi t-out 200
```

Related Commands

Command	Description
fddi c-min	Sets the C-Min timer on the PCM.
fddi tb-min	Sets the TB-Min timer in the PCM.
fddi tl-min-time	Controls the TL-Min time (the minimum time to transmit a PHY line state before advancing to the PCM state, as defined by the X3T9.5 specification).

fddi valid-transmission-time

To change the transmission valid timer (TVX) interval, use the**fddivalid-transmission-time** command in interface configuration mode. To revert to the default value, use the **no** form of this command.

fddi valid-transmission-time *microseconds* **fddi valid-transmission-time command**
no fddi valid-transmission-time

Syntax Description

microseconds	Number, in microseconds, that specifies the TVX interval. The range is from 2500 to 2147483647. The default is 2500.

Command Default

microseconds : 2500

Command Modes

Interface configuration

Command History

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

Usage Guidelines

Use this command to recover from a transient FDDI ring error by setting a longer transmission timer interval.

Examples

The following example shows how to change the transmission timer interval to 3000 microseconds:

```
Router(config)# interface fddi 0
Router(config-if)# fddi valid-transmission-time 3000
```

The following example shows how to change the transmission timer interval to 3000 microseconds on Cisco 7000 series routers or Cisco 7200 series routers:

```
Router(config)# interface fddi 3/0
Router(config-if)# fddi valid-transmission-time 3000
```

fdl

To set the Facility Data Link (FDL) exchange standard for CSU controllers or to set the FDL exchange standard for a T1 interface that uses the Extended Super Frame (ESF) framing format, use the **fdl** command in interface configuration mode. To disable FDL support or to specify that there is no ESF FDL, use the **no** form of this command.

Cisco 2600 Series and Cisco 3600 Series Routers
fdl {**att** | **ansi** | **all** | **none**}
no fdl {**att** | **ansi** | **all** | **none**}

Cisco 10000 Series Router
fdl {**att** | **ansi**}
no fdl {**att** | **ansi**}

Syntax Description

att	Specifies AT&T technical reference 54016 for ESF FDL exchange support.
ansi	Specifies ANSI T1.403 for ESF FDL exchange support.
all	Specifies both AT&T technical reference 54016 and ANSI T1.403 for ESF FDL exchange support.
none	Specifies that there is no support for ESF FDL exchange.

Command Default

ANSI T1.403 for ESF FDL exchange support

Command Modes

Interface configuration

Command History

Release	Modification
11.3	This command was introduced.
12.0(5)XK	The **none** keyword was added, and the **both** keyword was changed to **all**.
12.0(5)T	The **none** keyword was added, and the **both** keyword was changed to **all**.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(31)SB	This command was integrated into Cisco IOS Release 12.2(31)SB.
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 is available only for T1 links. This command sets the standard to be followed for FDL messaging through a 4-kbps out-of-band channel that a service provider uses to check for errors on the facility.

You must use the same FDL exchange standard as your service provider. If the setting is not correct, the link might not come up. You can configure a different standard on each T1 interface.

Note When using a multiport T1 ATM IMA network module on a Cisco 2600 series or Cisco 3600 series router, ESF framing and binary eight zero substitution (B8ZS) line encoding are supported. When using a multiport E1 ATM IMA network module on a Cisco 2600 series or Cisco 3600 series router, CRC4 multiframe framing and HDB3 line encoding are supported. These are the parameters specified by the ATM Forum, and they cannot be changed.

Examples

Cisco 2600 and Cisco 3600 Series Routers

The following example shows how to specify the ANSI standard and the AT&T standard for FDL exchange:

```
Router(config)# interface atm 0/2
Router(config-if)# fdl all
```

Cisco 10000 Series Router

The following example shows how to specify the AT&T standard for FDL exchange:

```
Router(config)# interface atm 1/0/0
Router(config-if)# fdl att
```

flowcontrol

To configure a port to send or receive pause frames, use the **flowcontrol** command in interface configuration mode. To return to the default settings, use the **no** form of this command.

flowcontrol {**send** | **receive**} {**desired** | **off** | **on**}
no flowcontrol {**send** | **receive**} {**desired** | **off** | **on**}

Syntax Description

send	Specifies that a port sends pause frames.
receive	Specifies that a port processes pause frames.
desired	Obtains predictable results regardless of whether a remote port is set to **on**, **off**, or **desired**.
off	Prevents a local port from receiving and processing pause frames from remote ports or from sending pause frames to remote ports.
on	Enables a local port to receive and process pause frames from remote ports or send pause frames to remote ports.

Command Default

Flow control is disabled.

Flow-control defaults depend upon port speed. The defaults are as follows:

- Gigabit Ethernet ports default to **off** for receive and **desired** for send.
- Fast Ethernet ports default to **off** for receive and **on** for send.
- On the 24-port 100BASE-FX and 48-port 10/100 BASE-TX RJ-45 modules, the default is **off** for receive and **off** for send.
- You cannot configure how WS-X6502-10GE 10-Gigabit Ethernet ports respond to pause frames. WS-X6502-10GE 10-Gigabit Ethernet ports are permanently configured to respond to pause frames.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.2(14)SX	This command was introduced on the Supervisor Engine 720.
12.2(17d)SXB	This command was implemented on the Supervisor Engine 2.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SCB	This command was integrated into Cisco IOS Release 12.2(33)SCB.

Usage Guidelines

The **send** and **desired** keywords are supported on Gigabit Ethernet ports only.

Pause frames are special packets that signal a source to stop sending frames for a specific period of time because the buffers are full.

Gigabit Ethernet ports on the Catalyst 6500 series switches and on the Cisco 7600 series routers use flow control to inhibit the transmission of packets to the port for a period of time; other Ethernet ports use flow control to respond to flow-control requests.

If a Gigabit Ethernet port receive buffer becomes full, the port transmits a “pause” packet that tells remote ports to delay sending more packets for a specified period of time. All Ethernet ports (1000 Mbps, 100 Mbps, and 10 Mbps) can receive and act upon “pause” packets from other devices.

You can configure non-Gigabit Ethernet ports to ignore received pause frames (disable) or to react to them (enable).

When used with the **receive**keyword, the **on** and **desired** keywords have the same result.

All the Gigabit Ethernet ports on the Catalyst 6500 series switches and the Cisco 7600 series routers can receive and process pause frames from remote devices.

To obtain predictable results, follow these guidelines:

- Use **sendon** only when remote ports are set to **receiveon** or **receivedesired**.
- Use **sendoff** only when remote ports are set to **receiveoff** or **receivedesired**.
- Use **receiveon** only when remote ports are set to **sendon** or **senddesired**.
- Use **sendoff** only when remote ports are set to **receiveoff** or **receivedesired**.

Examples

These examples show how to configure the local port to not support any level of flow control by the remote port:

```
Router# configure terminal

Router(config)# interface GigabitEthernet1/9 10.4.9.157 255.255.255.0

Router(config-if)# flowcontrol receive off
Router(config-if)# flowcontrol send off
```

Related Commands

Command	Description
show interfaces flowcontrol	Displays flow-control information.

frame-relay

To configure Frame Relay payload compression for each Frame Relay port, use the **frame-relay**command in interface configuration mode. To terminate this form of payload compression over Frame Relay, use the **no** form of this command.

frame-relay payload-compression frf9 stac caim [*element-number*]
no frame-relay payload-compression

Syntax Description

payload-compression	Packet-by-packet payload compression, using the Stacker method.
frf9 stac	Enables FRF.9 compression using the Stacker method. If the router contains a data compression Advanced Interface Module (AIM) for the Cisco 2600 series router, compression is performed in the hardware (hardware compression). If the compression Advanced Interface Module (CAIM) is not available, compression is performed in the software installed on the main processor of the router (software compression).
caim *element-number*	Enable the data compression AIM hardware compression daughtercard to do compression, at the element numbered beginning with 0 and incrementing to include all possible elements.

Command Default

Disabled

Command Modes

Interface configuration

Command History

Release	Modification
12.0(2)T	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

Use the **frame-relaypayload-compression** command to enable or disable payload compression on a point-to-point interface or subinterface. Use the **frame-relaymap** command to enable or disable payload compression on a multipoint interface or subinterface.

Shut down the interface before changing encapsulation types. Although this is not required, shutting down the interface ensures the interface is reset for the new encapsulation.

Examples

The following example shows Frame Relay configured to use payload compression with the frf9 stac algorithm for CAIM hardware compression, using the installed data compression AIM daughtercard as the compression source:

```
Router(config-if)# frame-relay payload-compression frf9 stac caim 0
```

Related Commands

Command	Description
compress stac caim	Specifies the exact hardware compression resource preferred.
encapsulation frame-relay	Enables Frame Relay encapsulation.
frame-relay interface-dlci	Assigns a DLCI to a specified Frame Relay subinterface on the router or access server.
frame-relay map	Defines mapping between a destination protocol address and the DLCI used to connect to the destination address.
show compress	Displays compression statistics.

framing

To select the frame type for the T1 or E1 data line, use the **framing** command in controller configuration mode.

T1 Lines
framing commandframing {**sfadm** | **esfadm**}

E1 Lines
framing {**crc4adm** | **pcm30adm** | **clear e1**}

Syntax Description

sfadm	Specifies super frame for the T1 channel.
esfadm	Specifies extended super frame for the T1 channel.
crc4adm	Specifies CRC4 framing mode for the E1 channel.
pcm30adm	Specifies CRC4 disabled framing mode for the E1 channel.
clear e1	Specifies clear-e1 framing mode for the E1 channel.

Command Default

Extended super frame (esf) for a T1 line CRC4 disabled framing (pcm30adm) for an E1 line

Command Modes

Controller configuration

Command History

Release	Modification
11.3	This command was introduced.
12.0(5)XE	The command was enhanced as an ATM interface configuration command.
12.0(7)XE1	This command was implemented on the Cisco 7100 series routers.
12.0(11)S	This command was integrated into Cisco IOS Release 12.0(11)S.
12.1(5)T	This command was integrated into Cisco IOS Release 12.1(5)T.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Use this command in configurations in which the router or access server is intended to communicate with T1 or E1 fractional data lines. The service provided determines which framing type is required for your T1 or E1 circuit.

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

Examples

The following example selects extended super frame as the T1 frame type:

```
Router(config)# controller t1 4/0
Router(config-controller)# framing esfadm
```

Related Commands

Command	Description
lbo	Specifies the distance of the cable from the routers to the network equipment.
linecode	Selects the line code type for a T1 or E1 line.

framing (CEM)

To specify the framing format of a circuit emulation (CEM) T1 or E1 port, use the **framing** command in controller configuration mode. To reset the framing format of the port to its default value, use the **no** form of this command.

T1 Port
framing {**sf** | **esf** | **unframed**}
no framing

E1 Port
framing {**crc4** | **no-crc4** | **unframed**}
no framing

Syntax Description

sf	Specifies that the T1 port framing format is set to super frame (SF) format, also commonly known as D4 framing format.
esf	Specifies that the T1 port framing format is set to extended super frame (ESF) format. This is the default for a T1 line.
crc4	Specifies that the E1 port framing format is set to the G.704 standard with the optional CRC4 mechanism defined in time slot 0 enabled. This is the default for a E1 line. For Cisco NCS 4200 Series, crc4 is the default framing mode for E1 interface module.
no-crc4	Specifies that the E1 port framing format is set to the G.704 standard with the optional CRC4 mechanism defined in time slot 0 disabled.
unframed	Specifies that no framing structure is sought (on the ingress data stream) or imposed (on the egress data stream) on the T1 or E1 port. For Cisco NCS 4200 Series, unframed is the default framing mode for T1 interface module.

Command Default

The framing format of a T1 line defaults to **esf**. The framing format of an E1 line defaults to **crc4**. If an unframed CEM channel is created on the port using the **cem-group** command, no framing structure is sought or imposed.

Command Modes

Controller configuration

Command History

Release	Modification
12.3(7)T	This command was introduced to support circuit emulation.
XE 3.18SP	This command was integrated in the Cisco NCS 4200 Series.
XE Everest 16.5.1	This command was integrated in the Cisco NCS 4200 Series and Cisco ASR 903 Series Router.

Usage Guidelines

Framing must be configured to match the framing format used by the attached equipment.

In order to change a line between unframed and any framed mode, you must first delete the CEM channels defined in the line.

Examples

The following example shows how to set the framing format of a CEM T1 port to be super frame format.

```
Router(config-controller)# framing
 sf
```

The following example shows how to set the framing format of a CEM E1 port to the G.704 standard with the optional CRC4 mechanism defined in time slot 0 disabled.

```
Router(config-controller)# framing no-crc4
```

Examples

The following example shows how to set the framing format of a CEM T1 port for Cisco NCS 4200 Series.

```
Router(config-controller)# framingunframed
```

Examples

The following example shows how to set the framing format of a CEM E1 port for Cisco NCS 4200 Series and Cisco ASR 903 Series Router.

```
Router(config-controller)# framingcrc4
```

Related Commands

Command	Description
cem-group	Creates CEM channels on T1 or E1 ports.

framing (E3 controller)

To specify the type of framing used by the E3 controller, use the **framing**command in controller configuration mode. To restore the default framing type, use the **no** form of this command.

framing {**bypass** | **g751**}
no framing

Syntax Description

bypass	Specifies that G.751 framing be bypassed.
g751	Specifies G.751 as the E3 framing type. This is the default.

Command Default

G.751 framing

Command Modes

Controller configuration

Command History

Release	Modification
11.1 CA	This command was introduced.
12.2(11)YT	This command was integrated into Cisco IOS Release 12.2(11)YT and implemented on the following platforms for E3: Cisco 2650XM, Cisco 2651XM, Cisco 2691, Cisco 3660 series, Cisco 3725, and Cisco 3745 routers.
12.2(15)T	This command was integrated into Cisco IOS Release 12.2(15)T.
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

If you do not specify the framing command, the default, **g751**, is used by the E3 controller to automatically determine the framing type received from the far-end equipment.

Configure framing as G.751 when the E3 connection terminates remotely on a Digital Link or Kentrox data service unit (DSU), or when needing a subrate on an E3 connection between two T3 or E3 network modules.

Note The local interface configuration must match the remote interface, or DSU, configuration.

When G.751 framing is used, DSU bandwidth can be used to select a payload subrate from 34,010 kbps down to 22 kbps.

When framing bypass is used, DSU bandwidth of 34,010 kbps must be configured.

When G.751 framing is used, configuring the scramble command can prevent some payload data from being mistakenly interpreted as G.751 framing bits by switches placed between the DSUs. By default, the no scramble command is configured.

When framing bypass is used, the no scramble command must be configured.

When G.751 framing is used, bit 11 of the G.751 frame is reserved for national use and is set to 1 by default. Configure national bit 1 only when required for interoperability with your telephone company.

Examples

The following example shows the framing for the E3 controller set to bypass:

```
Router(config)# controller e3 1/0
Router(config-controller)# framing bypass
```

Related Commands

Command	Description
scramble	Specifies the type of framing used by the T1 channels on the CT3IP in Cisco 7500 series routers.

framing (SONET)

To select the frame type of the frame received on an optical line, use the **framing**command in controller configuration mode.

framing {**sonet** | **sdh**}

Syntax Description

sonet	Specifies the framing type as SONET.
sdh	Specifies the framing type as Synchronous Digital Hierarchy (SDH).

Command Default

SONET is the default for the PA-MC-STM-1 port adapter. SDH is the default for the STM-1 trunk card.

Command Modes

Controller configuration

Command History

Release	Modification
12.0(14)S	This command was introduced.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(15)T	This command was integrated into Cisco IOS Release 12.2(15)T and support was added for the STM-1 trunk card on the Cisco AS5850 platform.
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.
XE Everest 16.5.1	This command was introduced on the Cisco ASR 920 Routers and Cisco NCS 4200 Series.

Usage Guidelines

Use this command to configure the framing type of the SONET controller. The PA-MC-STM-1 port adapter supports both the SONET and SDH framing modes. The STM-1 trunk feature card on the Cisco AS5850 supports only SDH framing.

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

Examples

The following example shows how to configure the framing type on a SONET controller of an STM-1 card in physical slot number 2 on a Cisco AS5850:

```
Router(config)# controller sonet 2/0
Router(config-controller)# framing sonet
```

Related Commands

Command	Description
show controllers sonet	Displays information about SONET controllers.

framing (T1 E1 controller)

To select the frame type for the T1 or E1 data line, use the **framing** command in controller configuration mode. To return to the default, use the **no** form of the command.

T1 Lines
framing {**sf** | **esf**}

E1 Lines
framing {**crc4** | **no-crc4**} [**australia**]

T1 Shared Port Adapter
framing {**sf** | **esf**}
no framing {**sf** | **esf**}

E1 Shared Port Adapter
framing {**crc4** | **no-crc4** | **unframed**}
no framing {**crc4** | **no-crc4** | **unframed**}

Syntax Description

sf	Specifies super frame as the T1 frame type. This is the default.
esf	Specifies extended super frame as the T1 frame type.
crc4	Specifies CRC4 as the E1 frame type. This is the default for Australia.
no-crc4	Specifies CRC4 disabled as the E1 frame type.
unframed	Specifies unframed mode.
australia	(Optional) Specifies the E1 frame type used in Australia.

Command Default

sf on a T1 line

crc4 on an E1 line

Command Modes

Controller configuration

Command History

12.2S	This command was integrated into Cisco IOS Release 12.2S.
12.2(25)S3	This command was integrated into Cisco IOS Release 12.2(25)S3.
12.2(18)SXE	This command was integrated into Cisco IOS Release 12.2(18)SXE to support SPAs on a Cisco 7600 series router and Catalyst 6500 series switch.
12.0(31)S	This command was integrated into Cisco IOS Release 12.0(31)S.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
15.1(2)SNH	This command was implemented on the Cisco ASR 901 Series Aggregation Services Routers.

Usage Guidelines

Use this command in configurations in which the router or access server is intended to communicate with T1 or E1 fractional data lines. The service provider determines the framing type required for your T1/E1 circuit.

To return to the default mode on a T1/E1 SPA, use the **no** form of this command. This command does not have a **no** form for other T1/E1 lines.

Examples

The following example selects extended super frame as the T1 frame type:

```
Router(config-controller)# framing esf
```

Related Commands

Command	Description
cablelength	Specifies the distance of the cable from the routers to the network equipment.
linecode	Selects the linecode type for T1 or E1 line.

framing (T3 controller)

To choose framing mode on a T3 port, use the **framing**command in controller configuration mode. To return to the default mode, use the no form of this command.

T3 Controllers
framing {**c-bit** | **m23**}
no framing

Channelized T3 Shared Port Adapters and the Cisco 7500 Series Routers with CT3IP Port Adapter
framing {**c-bit** | **m23** | **auto-detect**}
no framing

Syntax Description

auto-detect	Specifies detection of the framing type that it receives from the far-end equipment.
c-bit	Specifies that C-bit framing is used as the T3 framing type.
m23	Specifies that M23 framing is used as the T3 framing type.

Command Default

c-bit (for the 2-Port and 4-Port Channelized T3 SPA and most T3 controllers)

auto-detect (for the CT3IP in a Cisco 7500 series router)

Command Modes

Controller configuration

Command History

Release	Modification
11.1CA	This command was introduced.
12.2(11)YT	This command was integrated into Cisco IOS Release 12.2(11)YT and implemented on the following platforms for T3: Cisco 2650XM, Cisco 2651XM, Cisco 2691, Cisco 3660 series, Cisco 3725, and Cisco 3745 routers.
12.2(15)T	This command was integrated into Cisco IOS Release 12.2(15)T.
12.2S	This command was integrated into Cisco IOS Release 12.2S.
12.2(25)S3	This command was integrated into Cisco IOS Release 12.2(25)S3 to support SPAs on the Cisco 7304 routers.
12.2(18)SXE	This command was integrated into Cisco IOS Release 12.2(18)SXE to support SPAs on a Cisco 7600 series router or Catalyst 6500 series switch.
12.0(31)S	This command was integrated into Cisco IOS Release 12.0(31)S to support SPAs on the Cisco 12000 series routers.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

You can set the framing for each T1 channel by using the **t1framing**controller configuration command.

Cisco 7500 Series Routers with CT3IP Port Adapter

Because the CT3IP supports the Application Identification Channel (AIC) signal, the setting for the framing might be overridden by the CT3IP firmware.

Examples

The following example sets the framing mode on a T3 interface.

```
Router# configure terminal
Router(config)# controller t1 6/0/0
Router(config-controller)# framing m23
```

The following example sets the framing for the CT3IP to C-bit:

```
Router(config)# controller t3 9/0/0
Router(config-controller)# framing c-bit
```

Related Commands

Command	Description
controller	Configures a T1, E1, or T3 controller and enters controller configuration mode.
show controller	Displays controller configuration.
t1 framing	Specifies the type of framing used by the T1 channels.

framing (T3-E3 interface)

To choose framing mode on a T3 or E3 port, use the **framing**command in interface configuration mode. To return to the default mode, use the no form of this command.

PA-T3 and T3 Shared Port Adapters
framing {**bypass** | **c-bit** | **m13**}
no framing {**bypass** | **c-bit** | **m13**}

PA-E3 and E3 Shared Port Adapters
framing {**bypass** | **g751** | **g832**}
no framing {**bypass** | **g751** | **g832**}

Syntax Description

bypass	Bypasses DS3 framing mode.
c-bit	Enables DS3 C-bit framing mode.
m13	Enables DS3 M13 framing mode.
g751	Enables E3 G.751 framing mode.
g832	Enables E3 G.832 framing mode. The g832 keyword is not supported on Cisco 7304 routers with the 4-Port Clear Channel T3/E3 SPA.

Command Default

T3: C-bit framing

E3: g751 framing

Command Modes

Interface configuration

Command History

Release	Modification
11.1	This command was introduced.
12.2S	This command was integrated into Cisco IOS Release 12.2S.
12.2(25)S3	This command was integrated into Cisco IOS Release 12.2(25)S3 to support SPAs on the Cisco 7304 routers.
12.2(18)SXE	This command was integrated into Cisco IOS Release 12.2(18)SXE to support SPAs on a Cisco 7600 series router and Catalyst 6500 series switch. The **g832** keyword option was added to the command.
12.0(31)S	This command was integrated into Cisco IOS Release 12.0(31)S to support SPAs on the Cisco 12000 series routers.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

The default framing is described in the ITU-T Recommendation G.751.

Note The International Telecommunication Union Telecommunication Standardization Sector (ITU-T) carries out the functions of the former Consultative Committee for International Telegraph and Telephone (CCITT).

When the framing mode is **bypass**, the T3 frame data is not included in the T3 frame, just the data.

When the framing mode is **bypass**, the E3 frame data is not included in the E3 frame, just the data.

If you use the **bypass** keyword, scrambling must be set to the default (disabled), the DSU mode must be set to the default (0), and the DSU bandwidth must be set to the default (44736).

The g832 keyword is not supported on Cisco 7304 routers with the 2-Port and 4-Port Clear Channel T3/E3 SPA.

Examples

The following example sets the framing mode to bypass on interface 1/0/0:

```
Router(config)# interface serial 1/0/0
Router(config-if)# framing bypass
```

Related Commands

Command	Description
show controller serial	Displays serial line statistics.

full-duplex

To specify full-duplex mode on full-duplex single-mode and multimode port adapters, use the **full-duplex**command in interface configuration mode. To restore the default half-duplex mode, use the **no** form of this command.

full-duplex
no full-duplex

Syntax Description

This command has no arguments or keywords.

Command Default

Half-duplex; a Fast Ethernet Interface Processor (FEIP), and serial interfaces that are configured for bisynchronous tunneling

Autonegotiation

Command Modes

Interface configuration

Command History

Release	Modification
11.1	This command was introduced.
11.3	This command was modified to include information on FDDI full-duplex, single-mode, and multimode port adapters.
12.2(31)SB	This command was integrated into Cisco IOS Release 12.2(31)SB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Use this command if the equipment on the other end is capable of full-duplex mode.

This command specifies full-duplex mode on full-duplex single-mode and multimode port adapters available on the following networking devices:

- Cisco 7200 series routers
- Second-generation Versatile Interface Processors (VIP2s) in Cisco 7500 series routers
- FEIP ports
- Serial interface ports that uses bisynchronous tunneling

Refer to the *CiscoProductCatalog* for hardware compatibility information and for specific model numbers of port adapters.

To enable half-duplex mode, use the **nofull-duplex** or **half-duplex** command.

Note For the Cisco AS5300, the **duplexfull**| **halfauto**} command replaces the **full-duplex** and **half-duplex** commands. You will get the following error messages if you try to use the **full-duplex** and **half-duplex** commands on a Cisco AS5300: Router(config)# **interfacefastethernet0** Router(config-if)# **full-duplex** Please use duplex command to configure duplex mode Router(config-if)# Router(config-if)# **half-duplex** Please use duplex command to configure duplex mode

Support for This Command

Use the question mark (?) command to find out which port adapters support this command. If the interface does not support full-duplex, an informational message displayed, and no changes are made to the interface. To determine if the interface supports full-duplex, use the **showinterfaces**command. For example, the following message is displayed if the interface does not support full-duplex:

```
% interface does not support full-duplex.
```

Use on FDDI

Full-duplex on the FDDI full-duplex port adapters allows an FDDI ring with exactly two stations to transform the ring into a full-duplex, point-to-point topology. For the interface to operate in full-duplex mode, there must be only two stations on the ring, the two stations must be capable of operating in full-duplex mode, and both stations must complete a full-duplex autoconfiguration protocol. There is no FDDI token in full-duplex mode. Refer to the *CiscoProductCatalog* for specific model numbers of port adapters.

Full-duplex autoconfiguration protocol allows an FDDI station to dynamically and automatically operate in either half-duplex (or ring) or full-duplex mode, and ensures that the stations fall back to ring mode when a configuration change occurs, such as a third station joining the ring.

After booting the router, the FDDI stations begin operation in half-duplex mode. While the station performs the full-duplex autoconfiguration protocol, the station continues to provide data-link services to its users. Under normal conditions, the transition between half-duplex mode and full-duplex mode is transparent to the data-link users. The data-link services provided by full-duplex mode are functionally the same as the services provided by half-duplex mode.

If you change the full-duplex configuration (for example, from disabled to enabled) on supported interfaces, the interface resets.

Cisco 10000 Series Router

The Fast Ethernet line card responds only to 802.3x pause frames from another device when it autonegotiates the duplex mode (the default). The line card does not support 802.3x flow control when you manually set half-duplex or full-duplex mode.

Examples

Cisco 7200 Series Router

The following example configures full-duplex mode on the Cisco 7200 series routers:

```
Router(config)# interface fastethernet 0/1
Router(config-if)# full-duplex
```

Full-Duplex Binary Synchronous

The following example specifies full-duplex binary synchronous communications (Bisync) mode:

```
Router(config)# interface serial 0
Router(config-if)# encapsulation bstun
Router(config-if)# full-duplex
```

Full-Duplex on FDDI Interface

The following example enables full-duplex mode on FDDI interface 0:

```
Router(config)# interface fddi 0/1/0
Router(config-if)# full-duplex
```

Related Commands

Command	Description
half-duplex	Specifies half-duplex mode on an SDLC interface or on the FDDI full-duplex, single-mode port adapter and FDDI full-duplex, multimode port adapter on the Cisco 7200 series and Cisco 7500 series routers.
interface	Configures an interface type and enters interface configuration mode.
interface fastethernet	Selects a particular Fast Ethernet interface for configuration.
interface serial	Specifies a serial interface created on a channelized E1 or channelized T1 controller (for ISDN PRI, CAS, or robbed-bit signaling).
show interfaces	Displays statistics for all interfaces configured on the router or access server.
show interfaces fddi	Displays information about the FDDI interface.

g709 disable

To disable the ITU-T G.709 wrapper, use the **g709 disable** command in DWDM configuration mode. To enable the ITU-T G.709 wrapper, use the **no** form of this command.

g709 disable

no g709 disable

Syntax Description

Syntax Description

This command has no keywords or arguments.

Command Default

The G.709 wrapper is enabled.

Command Modes

DWDM configuration

Command History

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

Usage Guidelines

To display the G.709 alarms and counters, use the**show controller dwdm g709** command.

Examples

The G.709 wrapper is enabled by default. The following example shows how to disable the G.709 wrapper on an interface:

```
enable
configure terminal
controller dwdm 0/0/0
g709 disable
end
```

If you have disabled the G.709 wrapper using the **g709 disable** command, use the **no g709 disable** command to re-enable it, as shown in the following example:

```
enable
configure terminal
controller dwdm 0/0/0
no g709 disable
end
```

Related Commands

Command	Description
show controller dwdm	Displays DWDM controller configuration.

g709 fec

To configure the forward error correction (FEC) mode for the DWDM controller, use the **g709fec**command in controller configuration mode. To return to the default state, use the **no** form of this command.

g709 fec {**disable** | **enhanced** | **standard**}
no g709 fec

Syntax Description

disable	Disables FEC.
enhanced	Enables enhanced FEC mode.
standard	Enables standard FEC mode.

Command Default

Standard FEC mode is enabled by default.

Command Modes

Controller configuration (config-controller)

Command History

Release	Modification
12.2(33)SRD1	This command was introduced on the Cisco 7600 series router.

Usage Guidelines

The **g709fec** command can be used only when the DWDM controller is in the shutdown state.

Standard FEC is the default mode; therefore, if you use the **nog709fec** command, standard FEC is used.

Examples

The following example shows how to configure standard FEC mode on a DWDM controller:

```
Router(config)# controller dwdm 1/3
Router(config-controller)# g709 fec standard
```

Related Commands

Command	Description
controller dwdm	Configures a DWDM controller.
g709 odu threshold	Configures thresholds for selected ODU BER alarms.
g709 otu threshold	Configures thresholds for selected OTU BER alarms.
no g709 odu report	Disables the logging of selected ODU alarms.
no g709 otu report	Disables the logging of selected OTU alarms.
show controller dwdm	Displays ITU-T G.709 alarms, alerts, and counters.
transport-mode	Configures a transport mode.

g709 odu report

To enable the logging of selected optical channel data unit (ODU) alarms to the console for a DWDM controller, use the **g709odureport**command in controller configuration mode. To disable logging, use the no form of this command.

g709 odu report {**ais** | **bdi** | **lck** | **oci** | **pm-tca** | **ptim** | **sd-ber** | **sf-ber** | **tim**}
no g709 odu report {**ais** | **bdi** | **lck** | **oci** | **pm-tca** | **ptim** | **sd-ber** | **sf-ber** | **tim**}

Syntax Description

ais	Alarm indication signal reporting status.
bdi	Backward defect indication reporting status.
lck	Upstream connection locked reporting status.
oci	Open connection indication error reporting status.
pm-tca	Path monitoring BER TCA reporting status.
ptim	Payload type identifier mismatch reporting status.
sd-ber	Sets PM BER in excess of SD threshold reporting status.
sf-ber	Sets PM BER in excess of SF threshold reporting status.
tim	Sets Trace Identifier Mismatch reporting status.

Command Default

Logging is enabled for all keywords.

Command Modes

Controller configuration (config-controller)

Command History

Release	Modification
12.2(33)SRD1	This command was introduced on the Cisco 7600 series router.

Usage Guidelines

This command can be used only when the DWDM conroller is in the shutdown state.

Examples

The following example shows how to enable ODU reporting for OCI:

```
Router(config)# controller dwdm 1/2
Router(config-controller)# g709 odu report oci
```

Related Commands

Command	Description
controller dwdm	Configures a DWDM controller.
g709 fec	Configures the FEC for the DWDM controller.
g709 odu threshold	Configures thresholds for selected ODU BER alarms.

Command	Description
g709 otu threshold	Configures thresholds for selected OTU BER alarms.
show controller dwdm	Displays G.709 alarms, alerts, and counters.
show platform dwdm alarm history	Displays platform DWDM alarm history.

g709 odu overhead tti

To configure the Trail Trace Identifier (TTI) level for an Optical Channel Data Unit (ODU), use the **g709oduoverheadtti**command in DWDM configuration mode. To return to the default, use the **no** form of this command.

g709 odu overhead tti {**expected** | **sent**} {**ascii** | **hex**} *tti-string*
no g709 odu overhead tti {**expected** | **sent**} {**ascii** | **hex**} *tti-string*

Syntax Description

expected	Configures the expected TTI string.
sent	Configures the transmit TTI string.
ascii	Indicates that the string is in ASCII format.
hex	Indicates that the string is in hexidecimal format.
tti-string	The TTI level string. You can configure the TTI level string in ASCII string format or hexadecimal format. The ASCII text string can be a maximum of 64 characters. The hexadecimal string length must be an even number and can be a maximum of 128 bytes.

Command Default

No TTI level string is configured.

Command Modes

DWDM configuration.

Command History

Release	Modification
15.1(2)S	This command was introduced on the Cisco 7600 Router.

Usage Guidelines

To display the TTI strings, use the **showcontrollerdwdmg709** command.

Examples

The following example shows how to configure the expected TTI string:

```
Router(config)# controller dwdm 0/1/0/0
Router(config-dwdm)# g709 odu overhead tti expected ascii test_odu_5678
```

Related Commands

Command	Description
show controller dwdm	Displays optical parameters, G.709 alarms and counters, and register and module information for a DWDM controller.

g709 odu threshold

To configure thresholds for selected optical channel data unit (ODU) bit error rate (BER) alarms, use the **g709oduthreshold**command in controller configuration mode. To return to the default state, use the **no** form of this command.

g709 odu threshold {**pm-tca bit-error-rate** | **sd-ber bit-error-rate** | **sf-ber bit-error-rate**}
no g709 odu threshold {**pm-tca bit-error-rate** | **sd-ber bit-error-rate** | **sf-ber bit-error-rate**}

Syntax Description

pm-tca	Sets the path monitoring threshold crossing alert threshold.
sd-ber	Sets the signal degrade bit error rate (BER) threshold.
sf-ber	Sets the signal failure BER threshold.
bit-error-rate	Specifies the BER threshold value in the range from 3 through 9. The threshold value is interpreted as a negative exponent of 10 when determining the bit error rate. For example, a value of 5 implies a bit error rate of 10 to the minus 5. The default BER threshold value is 6.

Command Default

sd-ber: 6

sf-ber: 3

pm-tca: 3

Command Modes

Controller configuration (config-controller)

Command History

Release	Modification
12.2(33)SRD1	This command was introduced on the Cisco 7600 series router.

Usage Guidelines

This command can be used only when the DWDM controller is in the shutdown state.

Examples

The following example shows how to set the signal fail BER rate to 5:

```
Router(config)# controller dwdm 1/2
Router(config-controller)# g709 odu threshold sf-ber 5
```

Related Commands

Command	Description
controller dwdm	Configures a DWDM controller.
g709 fec	Configures the FEC for the DWDM controller
g709 otu threshold	Configures thresholds for selected OTU BER alarms.
no g709 odu report	Disables the logging of selected ODU alarms.
no g709 otu report	Disables the logging of selected OTU alarms.

Command	Description
show controller dwdm	Displays ITU-T G.709 alarms, alerts, and counters.
transport-mode	Configures a transport mode.

g709 otu report

To enable the logging of selected optical channel transport unit (OTU) alarms to the console for a DWDM controller, use the **g709otureport**command in controller configuration mode. To disable logging, use the no form of this command.

g709 otu report {**ais** | **bdi** | **iae** | **lof** | **lom** | **los** | **sm-tca** | **tim** | **sd-ber** | **sf-ber**}
no g709 otu report {**ais** | **bdi** | **iae** | **lof** | **lom** | **los** | **sm-tca** | **tim** | **sd-ber** | **sf-ber**}

Syntax Description

ais	Alarm indication signal reporting status.
bdi	Backward defect indication reporting status.
iae	Incoming alignment error reporting status.
lof	OTU loss of frame reporting status.
lom	Loss of multiple frame reporting status.
los	Loss of signal reporting status.
sm-tca	Section monitoring BER TCA reporting status.
tim	Trace identifier mismatch reporting status.
sd-ber	SM BER is in excess of the SD BER threshold
sf-ber	SM BER is in excess of the SF BER threshold

Command Default

Reporting is enabled for all keywords.

Command Modes

Controller configuration (config-controller)

Command History

Release	Modification
12.2(33)SRD1	This command was introduced on the Cisco 7600 series router.
XE 3.18SP	This command was introduced on the Cisco NCS 4200 Series router.

Usage Guidelines

This command can be used only when the DWDM controller is in the shutdown state.

Examples

The following example shows how to enable OTU reporting for IAE:

```
Router(config)# controller dwdm 1/2
Router(config-controller)# g709 otu report iae
```

Related Commands

Command	Description
controller dwdm	Configures a DWDM controller.

Command	Description
g709 fec	Configures the FEC for the DWDM controller.
g709 odu threshold	Configures thresholds for selected ODU BER alarms.
g709 otu threshold	Configures thresholds for selected OTU BER alarms.
no g709 odu report	Disables the logging of selected ODU alarms.
show controller dwdm	Displays ITU-T G.709 alarms, alerts, and counters.
show platform dwdm alarm history	Displays platform DWDM alarm history.
transport-mode	Configures a transport mode.

g709 otu threshold

To configure thresholds for selected optical channel transport unit (OTU) bit error rate (BER) alarms, use the **g709otuthreshold**command in controller configuration mode. To return to the default state, use the **no** form of this command.

g709 otu threshold sm-tca| sd-ber| sf-ber bit-error-rate
no g709 otu threshold sm-tca| sd-ber| sf-ber bit-error-rate

Syntax Description

sm-tca	Sets the Section Monitoring Threshold Crossing Alert threshold.
sd-ber	Sets the Signal Degrade Bit Error rate threshold.
sf-ber	Sets the Signal Failure Bit Error Rate threshold.
bit-error-rate	Sets the BER threshold value in the range from 3 through 9. The threshold value is interpreted as a negative exponent of 10 when determining the bit error rate. For example, a value of 5 implies a bit error rate of 10 to the minus 5. The default BER threshold value is 3.

Command Default

bit-error-rate: 3

Command Modes

Controller configuration (config-controller)

Command History

Release	Modification
12.2(33)SRD1	This command was introduced on the Cisco 7600 series router.
XE 3.18 SP	This command was introduced on the Cisco NCS 4200 Series router.

Usage Guidelines

This command can be used only when the DWDM controller is in the shutdown state.

Examples

The following example shows how to set the Section Monitoring Threshold Crossing Alert threshold to 5:

```
Router(config)# controller dwdm 1/2
Router(config-controller)# g709 otu threshold sm-tca 5
```

Related Commands

Command	Description
controller dwdm	Configures a DWDM controller.
g709 fec	Configures the FEC for the DWDM controller.
g709 odu threshold	Configures thresholds for selected ODU BER alarms.
no g709 odu report	Disables the logging of selected ODU alarms.
no g709 otu report	Disables the logging of selected OTU alarms.

Command	Description
show controller dwdm	Displays ITU-T G.709 alarms, alerts, and counters.
transport-mode	Configures a transport mode.

g709 tti-processing enable

To configure Trail Trace Identifier (TTI), use the **g709 tti-processing enable** command in the controller configuration mode.

g709 tti-processing enable {*odu* | *otu*}

Syntax Description

Syntax Description

odu	Configures TTI for selected ODU alarm.
otu	Configures TTI for selected OTU alarm.

Command Modes

Controller configuration

Command History

Release	Modification
15.6(02)SP	Support for this command was introduced on NCS 4200 Series router.

Usage Guidelines

The interface goes down in case of OTU TIM or ODU TIM alarms.

Examples

The following example shows how to enter CEM interface parameters:

```
enable
configure terminal
controller dwdm 0/4/1
shutdown
g709 tti-processing enable odu
no shutdown
end
```

Related Commands

Command	Description
clear controller dwdm	Displays the DWDM controller configuration.

gnss

To enable the global navigation satellite system (GNSS) module on the Cisco ASR 903, Cisco ASR 907, and the Cisco ASR 920 routers, use the **gnss** command in the global configuration mode.

gnss slot {*r0r1*}

Syntax Description

slot	Specifies the slot information.
r0	Indicates route processor slot 0.
r1	Indicates route processor slot 1.

Command Default

No default behavior or values.

Command Modes

Global configuration (config)

Command History

Release	Modification
IOS-XE 3.17	This command was introduced on the Cisco ASR 903, Cisco ASR 907, and the Cisco ASR 920 routers.

Usage Guidelines

This command enables the GNSS module on the router. However, you must execute the **no shutdown** command after the **gnss** command to ensure that the interface is administratively up.

Examples

The following example shows how to enable the GNSS module and enter the GNSS mode:

```
Router# configure terminal
Router(config)# gnss slot r0
Router(config-gnss)# no shutdown
```

Related Commands

Command	Description
1pps	Configures the pulse per second from the GNSS module.
anti-jam	Enables or disables the anti-jam mode on the GNSS module.
constellation	Configures the GNSS module based on the specified satellite constellations.
default	Resets the device to its default state.
exit	Exists the GNSS sub mode.
no	Negates the command or sets the value of the command to its default values.
shutdown	Enables GNSS module.

gtp

To enables Enhanced Wireless Access Gateway (EWAG) General packet radio service (GPRS) Tunneling Protocol (GTP) and enter EWAG GTP configuration mode, use the **gtp** command in global configuration mode.

gtp

Syntax Description

This command does not contain any keywords or arguments.

Command Default

This command has no defaults.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Release 3.8S	This command was introduced.

Examples

The following example shows how to enable GTP and configure parameters of an access point.

```
Device(config)# gtp
Device(config-gtp)# n3-request 3
Device(config-gtp)# interval t3-response 30
Device(config-gtp)# information-element rat-type wlan
Device(config-gtp)# interface local GigabitEthernet0/0/0
WARNING: same interface has already been configured
Device(config-gtp)# apn 1
Device(config-gtp-apn)#  apn-name starent.com
Device(config-gtp-apn)#  ip address ggsn 10.1.2.1
Device(config-gtp-apn)#  dns-server 10.1.2.1
Device(config-gtp-apn)#  dhcp-server 10.10.197.1
Device(config-gtp-apn)#  dhcp-lease 6000
Device(config-gtp-apn)#  tunnel mtu 1500
Device(config-gtp-apn)# end
```

Related Commands

Command	Description
apn	Configures an ASCII regular expression string to be matched against the APN for GPRS load balancing.
apn-name	Configures access point name.
debug gtp	Debugs information related to EWAG GTP.

Command	Description
dns-server	Specifies the DNS IP servers available to a DHCP client.
dhcp-server	Specifies a primary (and backup) DHCP server to allocate IP addresses to MS users entering a particular PDN access point.
dhcp-lease	Configures DHCP lease time in seconds.
interval (EWAG)	Configures message intervals.
information-element	Configures information elements.
interface (EWAG)	Configure EWAG interface.
ip address ggsn	Configures GGSN IP address.
n3-request	Specifies the maximum number of times that the quota server attempts to send a signaling request to the CSG.
show gtp	Displays information related to EWAG GTP.
tunnel mtu	Configures GTP tunnel parameters.

half-duplex

To specify half-duplex mode on an Synchronous Data Link Control (SDLC) interface or on the FDDI full-duplex, single-mode port adapter and FDDI full-duplex, multimode port adapter on the Cisco 7200 series and Cisco 7500 series routers, use the **half-duplex** command in interface configuration mode. To reset the interface to full-duplex mode, use the **no** form of this command.

half-duplex
no half-duplex

Syntax Description

This command has no arguments or keywords.

Command Default

Full-duplex mode is the default mode on an SDLC interface, the FDDI full-duplex, single-mode port adapter and FDDI full-duplex, multimode port adapter on the Cisco 7200 series and Cisco 7500 series routers.

Command Modes

Interface configuration

Command History

Release	Modification
11.1	This command was introduced.
11.3	This command was modified to include information on FDDI full-duplex, single-mode, and multimode port adapters.
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

SDLC Interfaces

The **half-duplex** command is used to configure an SDLC interface for half-duplex mode and is used on a variety of port adapters. Use the question mark (?) command to find out which port adapters support this command.

Note The **half-duplex**command replaces the **sdlchdx** and **media-typehalf-duplex** commands.

Note For the Cisco AS5300, the **duplexfullhalfauto**} command replaces the **full-duplex** and **half-duplex** commands. You will get the following error messages if you try to use the **full-duplex** and **half-duplex** commands on a Cisco AS5300: Router(config)# **interfacefastethernet0** Router(config-if)# **full-duplex** Please use duplex command to configure duplex mode Router(config-if)# Router(config-if)# **half-duplex** Please use duplex command to configure duplex mode

Enabling Full-Duplex Mode

To enable full-duplex mode, use the **nohalf-duplex**or**full-duplex**commands.

Note The **media-typehalf-duplex** command exists in Cisco IOS Release 11.0(5). As of Release 11.0(6), the keyword **half-duplex** was removed from the **media-type** command. In Release 11.0(6), the functionality for specifying half-duplex mode is provided by the**half-duplex** command.

Port Adapters

Refer to the *CiscoProductCatalog* for specific model numbers of port adapters.

Examples

The following example configures an SDLC interface for half-duplex mode:

```
Router(config-if)# encapsulation sdlc-primary
Router(config-if)# half-duplex
```

Related Commands

Command	Description
full-duplex	Specifies full-duplex mode on full-duplex single-mode and multimode port adapters.

half-duplex controlled-carrier

To place a low-speed serial interface in controlled-carrier mode, instead of constant-carrier mode, use the **half-duplexcontrolled-carrier**command in interface configuration mode. To return the interface to constant-carrier mode, use the **no** form of this command.

half-duplex controlled-carrier
no half-duplex controlled-carrier

Syntax Description

This command has no arguments or keywords.

Command Default

Constant-carrier mode, where Data Carrier Detect (DCD) is held constant and asserted by the DCE half-duplex interface.

Command Modes

Interface configuration

Command History

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

Usage Guidelines

This command applies only to low-speed serial DCE interfaces in half-duplex mode. Configure a serial interface for half-duplex mode by using the **half-duplex** command. Refer to the *CiscoProductCatalog* for specific model numbers of networking devices which support serial interfaces.

Controlled-carrier operation means that the DCE interface has DCD deasserted in the quiescent state. When the interface has something to transmit, it asserts DCD, waits a user-configured amount of time, then starts the transmission. When the interface has finished transmitting, it waits a user-configured amount of time and then deasserts DCD.

Examples

The following examples place the interface in controlled-carrier mode and then back into constant-carrier operation.

This example shows changing to controlled-carrier mode from the default of constant-carrier operation:

```
Router(config)# interface serial 2
Router(config-if)# half-duplex controlled-carrier
```

This example shows changing to constant-carrier operation from controlled-carrier mode:

```
Router(config)# interface serial 2
Router(config-if)# no half-duplex controlled-carrier
```

Related Commands

Command	Description
half-duplex	Specifies half-duplex mode on an SDLC interface or single-mode and multimode port adapters.
half-duplex timer	Tunes half-duplex timers.
physical-layer	Specifies the mode of a slow-speed serial interface on a router as either synchronous or asynchronous.

half-duplex timer

To tune half-duplex timers, use the **half-duplextimer** command in interface configuration mode. To return to the default parameter values, use the **no** form of this command.

half-duplex timer {**cts-delay** *value* | **cts-drop-timeout** *value* | **dcd-drop-delay** *value* | **dcd-txstart-delay** *value* | **rts-drop-delay** *value* | **rts-timeout** *value* | **transmit-delay** *value*}
no half-duplex timer {**cts-delay** *value* | **cts-drop-timeout** *value* | **dcd-drop-delay** *value* | **dcd-txstart-delay** *value* | **rts-drop-delay** *value* | **rts-timeout** *value* | **transmit-delay** *value*}

Syntax Description

cts-delay *value*	Specifies the delay introduced by the DCE interface from the time it detects the Request to Send (RTS) to the time it asserts Clear to Send (CTS) in response. The range is dependent on the serial interface hardware. The default **cts-delay** value is 0 ms.
cts-drop-timeout *value*	Determines the amount of time a DTE interface waits for CTS to be deasserted after it has deasserted RTS. If CTS is not deasserted during this time, an error counter is incremented to note this event. The range is from 0 to 1,140,000 ms (1140 seconds). The default **cts-drop-timeout** value is 250 ms.
dcd-drop-delay *value*	Applies to DCE half-duplex interfaces operating in controlled-carrier mode (see the **half-duplexcontrolled-carrier** command). This timer determines the delay between the end of transmission by the DCE and the deassertion of Data Carrier Detect (DCD). The range is from 0 to 4400 ms (4.4 seconds). The default **dcd-drop-delay** value is 100 ms.
dcd-txstart-delay *value*	Applies to DCE half-duplex interfaces operating in controlled-carrier mode. This timer determines the time delay between the assertion of DCD and the start of data transmission by the DCE interface. The range is from 0 to 1,140,000 ms (1140 seconds). The default **dcd-txstart-delay** value is 100 ms.
rts-drop-delay *value*	Specifies the time delay between the end of transmission by the DTE interface and deassertion of RTS. The range is from 0 to 1,140,000 ms (1140 seconds). The default **rts-drop-delay** value is 3 ms.
rts-timeout *value*	Determines the number of milliseconds the DTE waits for CTS to be asserted after the assertion of RTS before giving up on its transmission attempt. If CTS is not asserted in the specified amount of time, an error counter is incremented. The range is dependent on the serial interface hardware. The default **rts-timeout** value is 3 ms.
transmit-delay *value*	Specifies the number of milliseconds a half-duplex interface will delay the start of transmission. In the case of a DTE interface, this delay specifies how long the interface waits after something shows up in the transmit queue before asserting RTS. For a DCE interface, this dictates how long the interface waits after data is placed in the transmit queue before starting transmission. If the DCE interface is in controlled-carrier mode, this delay shows up as a delayed assertion of DCD. This timer enables the transmitter to be adjusted if the receiver is a little slow and is not able to keep up with the transmitter. The range is from 0 to 4400 ms (4.4 seconds). The default**transmit-delay** value is 0 ms.

Command Default

The default **cts-delay** value is 0 ms. The default **cts-drop-timeout** value is 250 ms. The default **dcd-drop-delay** value is 100 ms. The default **dcd-txstart-delay** value is 100 ms. The default **rts-drop-delay** value is 3 ms. The default **rts-timeout** value is 3 ms. The default**transmit-delay** value is 0 ms.

Command Modes

Interface configuration

Command History

Release	Modification
11.3	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

Tuning Half-Duplex Timers

The **half-duplextimer** command is used to tune half-duplex timers. With these timer tuning commands you can adjust the timing of the half-duplex state machines to suit the particular needs of their half-duplex installation.

You can configure more than one option using this command, but each option must be specified as a separate command.

Note The **half-duplextimercts-delay** command replaces the **sdlccts-delay** command. The **half-duplextimerrts-timeout** command replaces the **sdlcrts-timeout** command.

Value Ranges

The range of values for the **cts-delay** and **rts-timeout** keywords are dependent on the serial interface hardware.

Examples

The following example set the cts-delay timer to 10 ms and the transmit-delay timer to 50 ms:

```
Router(config)# interface serial 2
Router(config-if)# half-duplex timer cts-delay 10
Router(config-if)# half-duplex timer transmit-delay 50
```

Related Commands

Command	Description
half-duplex controlled-carrier	Places a low-speed serial interface in controlled-carrier mode, instead of constant-carrier mode.
physical-layer	Specifies the mode of a slow-speed serial interface on a router as either synchronous or asynchronous.

history (interface)

To enable an interface to maintain utilization history, use the **history** command in interface configuration mode. To disable an interface, use the **no** form of this command.

history {**bps** | **pps**} [*filter*]
no history

Syntax Description

bps	Maintains history in bits per second.
pps	Maintains history in packets per second.
filter	(Optional) Interface counters. See the table below for details. Any number of counters can be used.

Command Default

Interface utilization history is not maintained.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.2(33)XNE	This command was introduced.

Usage Guidelines

Once interface history is configured, the interface history histograms can be displayed using the **show interface history** command.

Some of the interface counters are interface-type-specific and cannot be specified unless they apply to the specific interface type being configured. Once interface history is configured, counters cannot be added or removed without first removing the interface history configuration.

Significant processor memory is allocated to maintain the history information. For example, if two counters are monitored, then approximately 4KB are used for the rate and counter history. If 20 counters are monitored, then approximately 19KB are used.

The table below lists the interface counter options for the **history (interface)** command.

Table 4: Interface Counter Options For Interface History

Interface Counter	Description
all	Includes all interface counters in the history.
babbles	Includes the Ethernet output babbles in the history.
crcs	Includes CRC counter in the history.
deferred	Includes the deferred Ethernet output in the history.
dribbles	Includes dribble counter in the history.
excessive-collisions	Includes Ethernet excessive output collisions in the history.
flushes	Includes flushes counter in the history.

Interface Counter	Description
frame-errors	Includes frame errors in the history.
giants	Includes giants counter in the history.
ignored	Includes ignored counter in the history.
input-broadcasts	Includes input broadcasts in the history.
input-drops	Includes input drops in the history.
input-errors	Includes input errors in the history.
interface-resets	Includes interface resets in the history.
late-collisions	Includes Ethernet late output collisions in the history.
lost-carrier	Includes Ethernet output lost carrier in the history.
multi-collisions	Includes Ethernet multiple output collisions in the history.
multicast	Includes Ethernet input multicast in the history.
no-carrier	Includes Ethernet output no-carrier in the history.
output-broadcasts	Includes output broadcasts in the history.
output-buffer-failures	Includes output buffer failures in the history.
output-buffers-swapped-out	Includes output buffers swapped out in the history.
output-drops	Includes output drops in the history.
output-errors	Includes output errors in the history.
output-no-buffer	Includes output no buffer in the history.
overruns	Includes overruns in the history.
pause-input	Includes Ethernet input pause in the history.
pause-output	Includes Ethernet output pause in the history.
runts	Includes runts in the history.
single-collisions	Includes Ethernet single output collisions in the history.
throttles	Includes throttles in the history.
underruns	Includes underruns in the history.
unknown-protocol-drops	Includes unknown protocol drops in the history.
watchdog	Includes Ethernet output watchdog in the history.

Examples

The following example shows how to configure the interface history command to maintain interface utilization history in bits per second (bps) and also the input-drop history:

```
Device(config-if)# history bps input-drops
```

Related Commands

Command	Description
show interface history	Displays information on the interface utilization.

hold-queue

To limit the length of the IP output queue on an interface, use the **hold-queue** command in interface configuration or template configuration mode. To restore the default values, use the **no** form of this command.

hold-queue *length* {**in** | **out**}
no hold-queue *length* {**in** | **out**}

Syntax Description

length	Integer that specifies the maximum number of packets in the queue. The range of valid values is from 0 to 65535.
in	Specifies the input queue. The default is 75 packets. For asynchronous interfaces, the default is 10 packets.
out	Specifies the output queue. The default is 40 packets. For asynchronous interfaces, the default is 10 packets.

Command Default

Input hold-queue limit is 75 packets. Output hold-queue limit is 40 packets. Asynchronous interfaces default is 10 packets.

Command Modes

Interface configuration (config-if)

Template configuration (config-template)

Command History

Release	Modification
10.0	This command was introduced.
11.1	The **nohold-queue**command was added.
12.2(14)SX	Support for this command was introduced on the Supervisor Engine 720.
12.2(17d)SXB	Support for this command on the Supervisor Engine 2 was extended to Cisco IOS Release 12.2(17d)SXB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SCB	This command was integrated into Cisco IOS Release 12.2(33)SCB.
15.1(2)T	This command was modified. The *length* argument was added to the **no** form of the command.
15.2(2)E	This command was integrated into Cisco IOS Release 15.2(2)E. This command is supported in template configuration mode.
Cisco IOS XE Release 3.6E	This command was integrated into Cisco IOS XE Release 3.6E. This command is supported in template configuration mode.

Usage Guidelines

Defaults

The default limits for this command prevent a malfunctioning interface from consuming an excessive amount of memory. There is no fixed upper limit to a queue size.

Back-to-Back Routing Updates

The default of 10 packets allows the Cisco IOS software to queue a number of back-to-back routing updates. This is the default for asynchronous interfaces only; other media types have different defaults.

Hold Queues and Priority Queueing

- The hold queue stores packets received from the network that are waiting to be sent to the client. Cisco recommends that the queue length not exceed10 packets on asynchronous interfaces. For most other interfaces, queue length should not exceed 100.
- The input hold queue prevents a single interface from flooding the network server with too many input packets. Further input packets are discarded if the interface has too many input packets outstanding in the system.
- If you are using priority output queueing, the length of the four output queues is set using the **priority-list** global configuration command. The **hold-queue** command cannot be used to set an output hold queue length in this situation.
- For slow links, use a small output hold-queue limit to prevent storing packets at a rate that exceeds the transmission capability of the link.
- For fast links, use a large output hold-queue limit. A fast link may be busy for a short time (and require the hold queue) but can empty the output hold queue quickly when capacity returns.
- You can display the current hold-queue setting and the number of packets that are discarded because of hold-queue overflows by using the **showinterfaces** command in user EXEC mode.



Caution Increasing the hold queue can have detrimental effects on network routing and response times. For protocols that use seq/ack packets to determine round-trip times, do not increase the output queue. Dropping packets instead informs hosts to slow down transmissions to match available bandwidth. This is generally better than having duplicate copies of the same packet within the network (which can happen with large hold queues).



Note When you use the **no** form of the **hold-queue** command, the *length* value (maximum number of packets in the queue) need not necessarily be the same as the configured value.

Examples

The following example shows how to set a small input queue on a slow serial line:

```
Router(config)# interface serial 0
Router(config-if)# hold-queue 30 in
```

The following example shows how to set an input value in an interface template:

```
Device# configure terminal
Device(config)# template user-template1
Device(config-template)# hold-queue 30 in
```

```
Device(config-template)# end
```

Cisco uBR10012 Universal Broadband Router

The following example shows how to modify the input hold queue on a Gigabit Ethernet SPA:

```
Router# configure terminal

Router(config)#interface GigabitEthernet3/0/0
Router(config-if)#hold-queue 30 in
```

Related Commands

Command	Description
priority-list	Establishes queueing priorities based on the protocol type.
show interfaces	Displays statistics for all interfaces configured on the router or access server.

hssi external-loop-request

To allow the router to support a CSU/DSU that uses the loopback circuit (LC) signal to request a loopback from the router, use the **hssiexternal-loop-request** command in interface configuration mode. To disable this function, use the **no** form of this command.

hssi external-loop-request
no hssi external-loop-request

Syntax Description

This command has no arguments or keywords.

Command Default

Disabled

Command Modes

Interface configuration

Command History

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

Usage Guidelines

The HSA applique on the High-Speed Serial Interface (HSSI) contains an LED that indicates the loopback circuit A (LA), loopback circuit B (LB), and LC signals that are transiting through the devices. The CSU/DSU uses the LC signal to request a loopback from the router. The CSU/DSU may want to do this so that its own network management diagnostics can independently check the integrity of the connection between the CSU/DSU and the router.

Use this command to enable a two-way, internal, and external loopback request on the HSSI from the CSU/DSU.



Caution If your CSU/DSU does not support this function, it should not be enabled on the router. Not enabling this function prevents spurious line noise from accidentally tripping the external loopback request line, which would interrupt the normal data flow.

Examples

The following example enables a CSU/DSU to use the LC signal to request a loopback from the router:

```
Router(config-if)# hssi external-loop-request
```

hssi internal-clock

To convert the High-Speed Serial Interface (HSSI) into a clock master, use the **hssiinternal-clock** command in interface configuration mode. To disable the clock master mode, use the **no** form of this command.

hssi internal-clock
no hssi internal-clock

Syntax Description

This command has no arguments or keywords.

Command Default

Disabled

Command Modes

Interface configuration

Command History

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

Usage Guidelines

Use this command in conjunction with the HSSI null-modem cable to connect two Cisco routers together with HSSI. You must configure this command at both ends of the link, not just one.

Note HSSI network module provides full-duplex connectivity at SONET OC-1/STS-1 (51.840 Mhz), T3 (44.736 MHZ), and E3 (34.368 MHz) rates in conformance with the EIA/TIA-612 and EIA/TIA-613 specifications. The actual rate of the interface depends on the external data service unit (DSU) and the type of service to which it is connected.

Examples

The following example shows how to convert the HSSI interface into a clock master:

```
Router(config-if)# hssi internal-clock
```

hub

To enable and configure a port on an Ethernet hub of a Cisco 2505 or Cisco 2507 router, use the **hub** command in global configuration mode.

hub ethernet *number port* [*end-port*]

Syntax Description

ethernet	Indicates that the hub is in front of an Ethernet interface.
number	Hub number, starting with 0. Because there is only one hub, this number is 0.
port	Port number on the hub. On the Cisco 2505 router, port numbers range from 1 to 8. On the Cisco 2507 router, port numbers range from 1 to 16. If a second port number follows, then this port number indicates the beginning of a port range.
end-port	(Optional) Last port number of a range.

Command Default

No hub ports are configured.

Command Modes

Global configuration

Command History

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

Usage Guidelines

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

Examples

The following example enables port 1 on hub 0:

```
Router# hub ethernet 0 1
Router(config-hub)# no shutdown
```

The following example enables ports 1 through 8 on hub 0:

```
Router# hub ethernet 0 1 8
Router(config-hub)# no shutdown
```

Related Commands

Command	Description
shutdown (hub)	Shuts down a port on an Ethernet hub of a Cisco 2505 or Cisco 2507 router.

hw-module boot

To specify the boot options for the module through the power management bus control register, use the **hw-moduleboot** command in privileged EXEC mode.

hw-module module *num* **boot** [*value*] {**config-register** | **eobc** | **flash** *image* | **rom-monitor**}

Syntax Description

module *num*	Specifies the number of the module to apply the command.
boot *value*	(Optional) Literal value for the module's boot option; valid values are from 0 to 15. See the “Usage Guidelines” section for additional information.
config-register	Boots using the module’s config-register value.
eobc	Boots using an image downloaded through EOBC.
flash *image*	Specifies the image number in the module’s internal Flash memory for the module’s boot option; valid values are 1 and 2.
rom-monitor	Stays in ROM-monitor mode after the module resets.

Command Default

This command has no default settings.

Command Modes

Privileged EXEC

Command History

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

Usage Guidelines

The valid values for the **boot***value* argument are as follows:

0--Specifies the module’s config-register value.

1--Specifies the first image in the Flash memory.

2--Specifies the second image in the Flash memory.

3--Stays in ROM-monitor mode after the module reset.

4--Specifies the download image through EOBC.

Examples

This example shows how to reload the module in slot 6 using the module’s config-register value:

```
Router# hw-module module 1 boot config-register
Router#
```

This example shows how to reload the module in slot 3 using an image downloaded through EOBC:

```
Router# hw-module module 1 boot eobc
Router#
```

Related Commands

Command	Description
showmodule	Displays the module status and information for all modules in the chassis.

hw-module energywise level

Note Effective with Cisco IOS Releases 15.1(1)T and 15.0.1M(2), the **hw-moduleenergywiselevel** command is not available in Cisco IOS software. For more information, see the Cisco 3900 Series, 2900 Series, and 1900 Series Software Configuration Guide .

To set the energywise level on the service module (SM), internal service module (ISM), or packet voice/data module (PVDM), use the **hw-moduleenergywiselevel**command in privileged EXEC mode.

hw-module *module-type* *slot-number* **energywise level** *level*

Syntax Description

module-type	Specifies the type of module.
slot-number	Specifies the slot, and if applicable, the sub slot number for the module.
energywise level	Specifies the power level for each module.
level	0-10. 0 will shut the power. Any number between 1 to 10 will turn the power on.

Command Default

The energywise level is 10.

Command Modes

Privileged EXEC (#)

Command History

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

Usage Guidelines

Use the **hw-moduleenergywiselevel**command in privileged EXEC mode to set the energywise level on the SM, ISM, or PVDM on your router. Specify the slot, and if applicable, the sub slot number for the module.

The energywise levelsupported for the module is specified by the module. The following table provides a definition for each energywise level:

Energywise Level	Definition
0	Shut
1	Hibernate
2	Sleep
3	Standby
4	Ready
5	Low

Energywise Level	Definition
6	Frugal
7	Medium
8	Reduced
9	High
10	Full



Note When the router reboots, the energywise level is set to energywise level 10 and will remain at energywise level 10 till a different energywise level is applied.

Examples

The following example shows how to set the energywise level at shut on an SM in slot 1.

```
Router#hw-module
sm 1
 energywise level
0
```

The following example shows how to set the energywise level at full on an SM in slot 1.

```
Router#hw-module
sm 1
 energywise level
10
```

Related Commands

Command	Description
show environment	To display temperature, voltage, fan, and power supply information, use the **showenvironment** command in user EXEC or privileged EXEC mode.
show platform hw-module-power	To display the energywise levels supported on the module, and the current and previous energywise level on the router, use the show platform hw-module-power command in user EXEC or privileged EXEC mode.

hw-module fan-tray version

To set the fan-type (high or low power) version, use the **hw-modulefan-trayversion**command in privileged EXEC mode.

hw-module fan-tray version [**1** | **2**]

Syntax Description

1 | **2**	(Optional) Specifies the version number; see the "Usage Guidelines" section for additional information.

Command Default

This command has no default settings.

Command Modes

Privileged EXEC

Command History

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

Usage Guidelines

Before you install a high-capacity fan tray, enter the **hw-modulefan-trayversion2** command to check for configuration problems, such as power-supply compatbility and power sufficiency. If there are no problems, a message is displayed to change the fan tray from version 1 to version 2. At this point, you can remove the old fan tray and quickly insert the new high-capacity fan tray.

The **hw-modulefan-trayversion2** command aplies to Cisco 7600 series routers configured with a Supervisor Engine 2. This command is not required in systems configured with a Supervisor Engine 720 or a Supervisor Engine 32.

This command is supported on the following chassis:

- WS-C6506
- WS-C6509
- WS-C6509-NEB/OSR7609

Set the version to **2** before installing higher power fan trays.

Set the version to **1** before downgrading to lower power fan trays.

Command confirmation does not change the fan power consumption or cooling capacity. It updates the backplane IDPROM. The new values take effect the next time that you insert a fan.

When you execute the command, the software checks the configurations and prompts for confirmation. Any illegal configurations (such as power-supply incompatibility) result in a warning being displayed and a command failure.

Examples

This example shows how to set the fan type for lower power fan trays:

```
Router#
hw-module fan-tray version 1
```

Related Commands

Command	Description
show environment cooling	Displays information about the cooling parameter.

hw-module interface als restart

To request a restart pulse when Automatic Laser Shutdown (ALS) restart mode is configured as manual, use the **h**w-module interface TenGigabitEthernet als restart command in Privileged EXEC mode.

hw-module interface TenGigabitEthernet slot/port als restart

Syntax Description

slot/port	Number of the chassis slot that contains the interface, where:
	• slot--Chassis slot number.
	• /port--Port number.
	  • For a 7600-ES+ITU-2TG, the valid values for the port are 1, 2.
	  • For a 7600-ES+ITU-4TG, the valid values for the port are 1, 2, 3, 4.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.2(33)SRD1	This command was introduced on the Cisco 7600 series router.

Examples

The following example shows how to request an ALS restart pulse for the Ten Gigabit Ethernet interface on slot 6 port number 2:

```
Router# hw-module interface TenGigabitEthernet 6/2 als restart
```

Related Commands

Command	Description
als	Enables the ALS mode.
als restart mode	Selects the ALS restart mode.
als restart pulse	Select the ALS pulse mode.
show als	Displays ALS status.
show controller dwdm	Displays G.709 alarms, alerts, and counters.
transport-mode	Configures a transport mode.

hw-module main-cpu qa error-recovery

To enable the recovery mechanism for a QA error condition on a Cisco 7500 series router, use the **hw-modulemain-cpuqaerror-recovery** command in global configuration mode. To disable the recovery mechanism for a QA error condition, use the **no** form of this command.

hw-module main-cpu qa error-recovery
no hw-module main-cpu qa error-recovery

Syntax Description

This command has no arguments or keywords.

Command Default

In Cisco IOS Release 12.0(24)S1, the recovery mechanism for a QA error condition is disabled; in all other releases, it is enabled.

Command Modes

Global configuration

Command History

Release	Modification
12.1(19)E	This command was introduced.
12.0(24)S1	This command was integrated into Cisco IOS Release 12.0(24)S1.
12.2(15)T5	This command was integrated into Cisco IOS Release 12.2(15)T5.
12.2(18)S	This command was integrated into Cisco IOS Release 12.2(18)S.
12.0(26)S	This command was integrated into Cisco IOS Release 12.0(26)S.
12.3(6)	This command was integrated into Cisco IOS Release 12.3(6).

Usage Guidelines

QA errors are sometimes seen in heavy traffic situations and may indicate a hardware failure or a software bug. In the case of a hardware failure, a Versatile Interface Processor (VIP) or a Route Switch Processor (RSP) must be replaced. It is possible, however, to recover from a QA error and not see another error for months. When the same buffer header is present in two different queues, the QA ASIC goes into an error condition and triggers a QA error interrupt. The QA error interrupt causes the RSP to dump the QA diagnostics and perform a cbus complex during which all the line cards are reloaded. Although the duplicate buffer header condition does not always indicate a hardware failure, the downtime of up to 300 seconds creates a real problem in the network.

The **hw-modulemain-cpuqaerror-recovery** command has been created to enable a recovery mechanism for a QA error by allowing the router to remove the duplicate buffer header from the queue that shows the problem and requeue the buffer header. By using the QA error recovery, the downtime is reduced to less than one second under lab conditions. Three QA errors caused by buffer headers are permitted before the router performs a cbus complex and reloads all the line cards.

After three QA errors caused by duplicate queued buffer headers occur, the cbus complex is initiated and the line cards reload. Other QA errors, such as a null buffer header on any queue, can occur. Recovery is not possible in these cases, and the QA error triggers a cbus complex and subsequent line-card reloads. The QA error condition is specific to the Cisco 7500 series routers.

Examples

The following example shows how to enable the QA error recovery mechanism when a Cisco IOS Release 12.0(24)S1 image is used on a Cisco 7500 series router. In all other supported releases, the QA error recovery mechanism is enabled by default.

```
Router(config)# hw-module main-cpu qa error-recovery
```

Related Commands

Command	Description
show controllers cbus	Displays information about the cBus controller card.

hw-module mode

To configure the interface module from 10G to 5G mode, use the **hw-module mode** command in global configuration mode.

hw-module *slot* / *bay PID***mode** *mode*

Use the following command to disable the eight unused odd ports (1, 3, 5, 7, 9, 11, and 15) of A900-IMA8CS1Z-M interface modules within the slots of Cisco N560-RSP4 and Cisco N560-RSP4-E routers:

hw-module *slot 0-15* **im-mode** *1*

Syntax Description

Syntax Description:

slot	Physical slot number of the interface
bay	Bay of the interface
PID	Part number of the interface modules
mode	Option to select the mode of the interface module
mode	Selected mode of the Interface Module, for example 5G_CEM.

Command Default

Default is 10G mode

Command Modes

Global configuration

Command History

Release	Modification
XE Everest 16.5.1	This command was introduced into the Cisco NCS 4200 Series, NCS 560 Series, and Cisco ASR 900 Series Routers.

Usage Guidelines

We recommend that you remove all the configurations before configuring 5G mode for the interface module. Do not use the **mode** keyword if you want to configure 10G mode.

Note Only 4-port-only mode is supported on the 8-port 10 Gigabit Ethernet Interface Module (8x10GE) interface module.

Examples

The following example shows how to configure configure 5G mode from 10G mode:

```
enable
configure terminal
platform hw-module configuration
hw-module 0 / 3 PID mode 5G_CEM
end
```

The following example shows the configuration of 8-port 10 Gigabit Ethernet Interface Module (8x10GE) interface module:

```
Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# platform hw-module configuration
Router(conf-plat-hw-conf)# hw-module 0/3 A900-IMA8Z mode ?
  4-ports-only  Four Ports

Router(conf-plat-hw-conf)#hw-module 0/3 A900-IMA8Z mode 4-ports-only

Interface configs would be defaulted before mode change?? [yes/no]: yes
```

Related Commands

Command	Description
show running-config | include mode	Verifies if the interface module is configured in 5G mode.

hw-module oversubscription

To administratively disable the oversubscribed ports (3, 4, 7, and 8) on a module, use the **hw-moduleoversubscription** command. Use the **no** form of this command to enable the oversubscribed ports.

hw-module module *num* **oversubscription**
no hw-module module *num* **oversubscription**

Syntax Description

module *num*	Applies the command to a specific module.

Command Default

Oversubscription is enabled by default.

Command Modes

Global configuration

Command History

Release	Modification
12.2(18)ZY	Support for this command was introduced (Cisco 76700 series router).
12.2(18)SXF5	Support for this command was intruduced (Catalyst 6500 series switch).

Usage Guidelines

This command is supported on the WS-X6708-10G-3C and the WS-X6708-10G-3CXL modules only.

When you disable the oversubscribed ports, the port is put into shutdown mode. In this mode, you cannot enter the **noshut** command on the disabled ports. If you attempt to enter the **noshut** command on the disabled ports, this message appears:

```
The current module is operating in non-oversubscription mode. To utilise this interface,
enable oversubscription mode for the module.
```

When you enter the **showinterfaces** command on the disabled ports, the output displays “disabled for performance” to distinguish between the normal port shutdown and the shutdown for performance.

Examples

This example shows how to administratively disable the oversubscribed ports on a module:

```
Router #
hw-module module 3 oversubscription
Router #
```

This example shows how to administratively enable the oversubscribed ports on a module:

```
Router #
no hw-module module 3 oversubscription
Router #
```

Related Commands

Command	Description
show interfaces	Displays traffic that is seen by a specific interface.

hw-module power-supply power-cycle

To power cycle the power supplies, use the **hw-modulepower-supplypower-cycle**command in privileged EXEC mode.

hw-module power-supply {1 | 2} power-cycle

Syntax Description

1 | 2	Specifies the power supply to power cycle.

Command Default

This command has no default settings.

Command Modes

Privileged EXEC (#)

Command History

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

Usage Guidelines

If you have redundant power supplies and you power cycle one of the power supplies, only that power supply is power cycled. If you power cycle both power supplies, the system goes down and comes back up in 10 seconds.

If you only have one power supply and you power cycle that power supply, the system goes down and comes back up in 10 seconds.

This command works only on routers with an 8700 watt power supply.

Examples

This example shows how to power cycle a power supply:

```
Router# hw-module power-supply 2 power-cycle
Power-cycling the power supply may interrupt service.
Proceed with power-cycling? [confirm]
Power-cycling power-supply 1
22:10:23: %C6KPWR-SP-2-PSFAIL: power supply 1 output failed.
22:10:25: %C6KENV-SP-4-PSFANFAILED: the fan in power supply 1 has failed
22:10:33: %C6KPWR-SP-4-PSOK: power supply 1 turned on.
22:10:33: %C6KENV-SP-4-PSFANOK: the fan in power supply 1 is OK
Router#
```

hw-module pxf stall-monitoring

To enable the parallel express forwarding (PXF) stall monitor on the Cisco 10000 series router, and configure the default threshold values for resetting the line card (LC) and the Hyper Transport Data Protocol (HTDP), use the **hw-modulepxfstall-monitoring**command in the global configuration mode. To disable the PXF stall monitor, use the **no** form of this command.

hw-module pxf stall-monitoring [**HT-Reset** *threshold-value* | **LC-Reset** *threshold-value*]
no hw-module pxf stall-monitoring [**HT-Reset** *threshold-value* | **LC-Reset** *threshold-value*]

Syntax Description

HT-Reset *threshold-value*	Specifies the threshold value for HTDP reset. The valid value ranges from 4 to 6. By default, the threshold value is set to 3.
LC-Reset *threshold-value*	Specifies the threshold value for LC reset. The valid value ranges from 4 to 6. By default, the threshold value is set to 3.

Command Default

None

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(33)XNE	This command was introduced.

Usage Guidelines

Initially, use the **hw-modulepxfstall-monitoring**command to enable the PXF stall monitor on the Cisco 10000 series router. Then use the **hw-modulepxfstall-monitoring**command again, to configure the threshold values of LC and HTDP reset.

Examples

The following example shows how to enable the PXF stall monitor, and configure the threshold values of LC and HTDP reset, using the **hw-modulepxfstall-monitoring**command.

```
Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# hw-module pxf stall-monitoring
Router(config)# hw-module pxf stall-monitoring HT-Reset 5
Router(config)# hw-module pxf stall-monitoring LC-Reset 4
```

Related Commands

Command	Description
show pxf stall-monitoring	Displays the current configuration and the operating status of the PXF stall monitor.

hw-module reset

To reset a module by turning the power off and then on, use the **hw-module reset** command in privileged EXEC mode.

hw-module module *num* **reset**

Syntax Description

module *num*	Applies the command to a specific module; see the "Usage Guidelines" section for valid values.

Command Default

This command has no default settings.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(14)SX	This command was introduced on the Supervisor Engine 720.
12.2(17d)SXB	This command on the Supervisor Engine 2 was extended to Release 12.2(17d)SXB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(31)SB2	This command was integrated into Cisco IOS 12.2(31)SB2.

Usage Guidelines

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

Examples

This example shows how to reload a specific module:

```
Router#
hw-module module 3 reset
```

hw-module sec-cpu reset

To reset and reload the standby Route Switch Processor (RSP) with the specified Cisco IOS image and to execute the image, use the **hw-modulesec-cpureset** command in privileged EXEC mode.

hw-module sec-cpu reset

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.0(16)ST	This command was introduced.
12.0(19)ST1	This command was enabled in privileged EXEC mode.
12.0(22)S	This command was integrated into Cisco IOS Release 12.0(22)S.
12.2(4)XF	This command was integrated into Cisco IOS Release 12.2(4)XF on the Cisco uBR10012 router.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.3(7)T	This command was integrated into Cisco IOS Release 12.3(7)T.
12.3BC	This command was integrated into Cisco IOS Release 12.3BC.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(31)SB2	This command was integrated into Cisco IOS Release 12.2(31)SB2.
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

Before using this command, you must use the **hw-moduleslotimage**global configuration command to specify a high availability Cisco IOS image to run on the standby RSP. After the high availability image is loaded in the active RSP, use the **hw-modulesec-cpureset** command to reset and reload the standby RSP with the specified Cisco IOS image and to execute the image. To load the standby RSP with the default micro-IOS software contained in the active RSP image instead of a high availability Cisco IOS image, use the **no** form of the **hw-moduleslotimage** command followed by the **hw-modulesec-cpureset**command.

Examples

The following example shows a Cisco 7513 router with the standby RSP loaded in slot 7. The standby RSP is reset and reloaded with the rsp-pv-mz high availability Cisco IOS image. Both RSPs have slot 0 flash memory cards.

```
Router(config)# hw-module slot 7 image slot0:rsp-pv-mz
Router(config)# end
Router# hw-module sec-cpu reset
```

Related Commands

Command	Description
hw-module slot image	Specifies a high availability Cisco IOS image to run on an active or standby RSP.

hw-module shutdown

To shut down the module, use the **hw-module shutdown** command in privileged EXEC mode.

hw-module module *num* **shutdown**

Syntax Description

module *num*	Applies the command to a specific module; see the "Usage Guidelines" section for valid values.

Command Default

This command has no default settings.

Command Modes

Privileged EXEC

Command History

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

Usage Guidelines

This command is supported on the SSL Services Module and the NAM.

If you enter the hw-module **shutdown**command to shut down the module, you will have to enter the no power enable module command and the **power enable module** command to restart (power down and then power up) the module.

Examples

This example shows how to shut down and restart the module:

```
Router# hw-module module 3 shutdown
Router# no power enable module 3
Router# power enable module 3
```

hw-module simulate link-up

To enable softlink on a specified module, use the **hw-modulesimulatelink-up**command in privileged EXEC mode. For information on disabling softlink, refer to the "Usage Guidelines" section.

hw-module module *num* **simulate link-up**

Syntax Description

module *num*	Applies the command to a specific module; see the "Usage Guidelines" section for valid values.

Command Default

This command has no default settings.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(18)SXD	Support for this command was introduced on the Supervisor Engine 720 and the Supervisor Engine 2.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

This command is supported on Ethernet modules only.

To disable softlink on a module, you must perform one of the following procedures:

- Enter the **shutdown** and then the **noshutdown**commands on all the ports on the module.
- Enter the **hw-modulereset**command.

When you apply this command to a module, the port LEDs on the module will glow green and simulate a link-up condition. This command can be used for testing interface configurations without cabling to the interface.

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

Examples

This example shows how to enable softlink on a module:

```
Router# hw-module module 3 simulate link-up
Router#
```

Related Commands

Command	Description
hw-module reset	Resets a module by turning the power off and then on.

hw-module slot

T o enable the router shelf to restart a stopped Dial Shelf Controller (DSC) card, to stop a DSC card, or to cause a shutdown, reset, or reload of any specified dial shelf feature board, use the **hw-moduleslot**command in privliged EXEC mode and global configuration mode.

hw-module slot *shelf-id/slot-number* {**reload** | **reset** | **shutdown** {**powered** | **unpowered**} [**dual-wide**] | **start** | **stop**}

Syntax Description

shelf-id	Number of the dial shelf. The default number for the dial shelf is 1.
/ *slot-number*	Number of the slot in the shelf where the target feature board or DSC is installed. If the **start** or **stop** keyword is used, the slot number must be either 12 or 13, because these keywords apply only to DSCs.
reload	Enables a remote reload of an individual feature board without having to use manual online insertion and removal (OIR).
reset	Resets a feature board.
shutdown	Shuts down a feature board.
powered	Shuts down the DSC and all of its interfaces and leaves them in an administratively down state with power enabled.
unpowered	Shuts down the DSC and all of its interfaces and leaves them in an administratively down state without power.
dual-wide	(Optional) Specifies the dual-wide port adapter (PA).
start	Restarts the specified DSC.
stop	Stops the specified DSC.

Command Default

Shuts down the DSC and all of its interfaces and leaves them in an administratively down state with power enabled.

Command Modes

Global configuration (config) Privileged EXEC (#)

Command History

Release	Modification
11.3(6)AA	The **hw-module** command was introduced.
12.1	• The **hw-module** command was expanded to become the **hw-moduleslot**command. • The **reload** keyword was added to enable a remote reload of a feature board.
12.3(2)T	The**reset**and **shutdown** keywords were added.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Release	Modification
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.
12.2(31)SB	This command was integrated into Cisco IOS Release 12.2(31)SB.
12.2(33)SB	This command's behavior was modified on the Cisco 10000 series router for the PRE3 and PRE4, and the **reload** option was introduced on the router.
15.0(1)M	This command was modified. The command became available in global configuration mode. The **powered**, **unpowered**, and **dual-wide** keywords were added.

Usage Guidelines

The **stop** form of this command is issued from the router shelf console instead of by pressing the attention (ATTN) button on the target DSC. Confirmation of when the start or stop took place is displayed. Warnings are issued and confirmation input is required if a **stop** command will result in a loss of service when backup functionality is not available.

When a DSC card is stopped, removed, and then reinstalled, there is no need to restart the card (whether the card is the original or a replacement) because a freshly installed card reboots as the backup DSC automatically. However, if a DSC is stopped, either by using the ATTN button or by issuing the **hw-moduleslotstop** command, it must be restarted by using the **start** form of the same command, or the DSC must be removed and reinstalled in order to reboot.

Press the ATTN button on the DSCs to shut down a card manually before removing the card. This is equivalent to issuing an **hw-moduleslot** command for that card at the router command prompt. Use the ATTN button to shut down the card before it is swapped out or tested in place, or to restart it, if the card has not been removed after having been shut down.

Tip The **hw-module** slot *shelf-id*/*slot-number***reload** form of this command is useful for simulating an OIR event in the case of a feature board failure when physical access to the feature board card is restricted.

Entering the **hw-module** slot *shelf-id*/*slot-number***reload**command initiates the feature board reload process through power cycling. The **hw-module** slot *shelf-id*/*slot-number***reload** command cannot be used to reload DSCs.

Use the **reset** form of this command to reset the specified feature card and drop all active calls.

Use the **shutdown** form of this command to shut down the specified feature card and drop all active calls.

Cisco 10000 Series Router Usage Guidelines,

In Cisco IOS Release 12.2(33)SB, when you enter the **hw-moduleslot***slot-number***reset** command, the software asks you to confirm the command.

In Cisco IOS Release 12.2(31)SB, the software does not ask you to confirm the **hw-moduleslot***slot-number***reset** command.

Examples

The following example shows how to stop the DSC in slot 13 and start the other DSC in slot 12 (which was previously stopped):

```
Router# hw-module slot 1/13 stop
Router# hw-module slot 1/12 start
```

The following example shows how to reload the dial shelf feature board in slot 6:

```
Router# hw-module slot 1/6 reload
```

The following example shows how to reset the card in slot 3:

```
Router# hw-module slot 1/3 reset
```

The following example shows how to shut down the PRE card located in slot 3:

```
Router# hw-module slot 1/3 shutdown powered
```

Related Commands

Command	Description
debug redundancy	Displays information used for troubleshooting dual (redundant) DSC cards.
show redundancy	Displays current or historical status and related information on dual (redundant) DSC cards.

hw-module slot (6500)

To enable ports on a module, use the **hw-moduleslot** command. To disable ports on a module, use the **no** form of this command.

hw-module slot *num* {**clear-block** | **oversubscription**} [**port-group** *num*]
no hw-module slot *num* {**clear-block** | **oversubscription**} [**port-group** *num*]

Syntax Description

slot *num*	Applies the command to a specific module.
clear-block	Drops the packets that are destined for jammed ports and continues delivering the packets for other ports.
oversubscription	Administratively disables the oversubscribed ports on a module. To enable oversubscription, use the **no** form of this command.
port-group *num*	(Optional) Applies the command to a specific port group on the module. The range depends on the module type.

Command Default

The default settings are as follows:

- Clear block is enabled by default.
- Oversubscription is enabled by default.

Command Modes

Global configuration

Command History

Release	Modification
12.2(18)SXF5	Support for this command was introduced (Catalyst 6500 series switch).
12.2(33)SXH1	Support for these keywords and arguments were introduced: • clear-block [port-group *num* • oversubscription [port-group *num*
12.2(33)SXH2	This command was changed to support the following modules: • WS-X6716-10G-3C • WS-X6716-10G-3CXL

Usage Guidelines

This command is supported on the following modules:

- WS-X6708-10G-3C--The port-group *num* and the clear-block keywords and argument are not supported.
- WS-X6708-10G-3CXL--The port-group *num* and the clear-block keywords and argument are not supported.
- WS-X6716-10G-3C

- WS-X6716-10G-3CXL

When you disable the oversubscribed ports, the port is put into shutdown mode. In this mode, you cannot enter the **noshut** command on the disabled ports. If you enter the **noshut** command on the disabled ports, this message appears:

```
The current module is operating in non-oversubscription mode. To utilise this interface,
enable oversubscription mode for the module.
```

When you enable oversubscription for a port group, the port group is in mux mode. When you disable oversubscription, the port group is in transparent mode. When a group is in transparent mode, the first port in the group retains its administrative status and the remaining three ports are administratively shut down. You cannot enter the **shut**, and then the **noshut** commands on the disabled ports. You can enter the **shut**, and then the **noshut** commands on the enabled port in the group.

The port-group mappings for the WS-X6716-10G-3C and the WS-X6716-10G-3CXL modules are as follows:

- Group 1--Ports 1 to 4. Port 1 is enabled in transparent mode.
- Group 2--Ports 5 to 8. Port 5 is enabled in transparent mode.
- Group 3--Ports 9 to 12. Port 9 is enabled in transparent mode.
- Group 4--Ports 13 to 16. Port 13 is enabled in transparent mode.

For the WS-X6716-10G-3C and the WS-X6716-10G-3CXL modules in transparent mode, ports 2, 3, 4, 6, 7, 8, 10, 11, 12, 14, 15, 16 are disabled.

If you specify a slot number without a group number, all four groups are put into transparent/mux mode.

You cannot put the port group into oversubscription mode when any port in the port group is configured as a virtual switch link (VSL). A warning message is displayed asking you to disable the VSL link before changing to oversubscription mode.

When you enter the **showinterfaces** command on the disabled ports, the output displays “disabled for performance” to distinguish between the normal port shutdown and the shutdown for performance.

Each 4-port group shares a common packet queue. If head-of-line blocking is enabled and one port of the four ports receives a pause frame, all packets are blocked behind this packet until the packet is delivered to the flow-controlled port. You can enter the **hw-moduleslot**clear-block [port-group *num*] command to drop the packets that are destined for the jammed port and continue to deliver the packets for other ports.

Examples

This example shows how to administratively disable the oversubscribed ports on a module:

```
Router#
no hw-module slot 3 oversubscription
Router#
```

This example shows how to administratively disable the oversubscribed ports on a specific port group:

```
Router#
no hw-module slot 3 oversubscription port-group 4
Router#
```

This example shows how to administratively enable the oversubscribed ports on a module:

```
Router#
hw-module slot 3 oversubscription
Router#
```

This example shows how to drop the packets that are destined for the jammed port and continue to deliver the packets for other ports:

```
Router#
hw-module slot 3 clear-block port-group 4
Router#
```

Related Commands

Command	Description
show interfaces	Displays traffic that is seen by a specific interface.
show hw-module slot	Displays information for a SPA interface processor (SIP) or other module.

hw-module slot (7300)

To prepare a line card, MSC, or PCI port adapter carrier card for online removal, use the**hw-moduleslot** command in privileged EXEC mode.

hw-module slot *slot-number* {**stop** | **start**}

Syntax Description

slot-number	Specifies the slot number of the line card, MSC, or PCI port adapter carrier card.
stop	Stops traffic, turns on the OIR LED, shuts down all interfaces, and deactivates the line card, MSC, or PCI port adapter carrier card.
start	Restarts the line card and shuts off the OIR LED, putting the hardware back online.

Command Default

No default behavior or values.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.1(9)EX	This command was enabled on the Cisco 7304 router.
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

Use the **hw-moduleslot***slot-number***stop**command to stop traffic, turn on the green OIR LED, and shut down all interfaces to remove a line card, MSC, or PCI port adapter carrier card from the Cisco 7304 router without disrupting data flow. You should not remove hardware while traffic is still running.

The **stop** keyword stops traffic through interfaces and deactivates the hardware. When the OIR LED turns green, the hardware has been deactivated and can be physically removed.

The **hw-moduleslot***slot-number***start**command restarts the line card, MSC, or PCI port adapter carrier card and shuts off the OIR LED, putting the card back online.

Use the **hw-moduleslot***slot-number***start**command if you issue the **hw-moduleslot***slot-number***stop** command, did not remove the hardware, and now want to reactivate it. If you remove and then reinsert the hardware, the hardware restarts without this command.

This command cannot be used for online removal of SPAs. For online removal of SPAs, use the **hw-modulesubslot** command.

You can also use thiscommand to restore a line card, MSC, or PCI port adapter carrier card that has been deactivated due to some failure.

Note Line cards, MSCs, and PCI port adapter carrier cards are automatically initialized after being inserted or after a system bootup. You do not need to issue the**hw-moduleslot***slot-number***start** command.

Examples

The following example shows how to deactivate the line card, MSC, or PCI port adapter carrier card in slot 2. After entering this command and the green OIR LED turns on, you can remove the hardware and insert a new piece of hardware:

```
Router# hw-module slot 2 stop
```

The following example shows how to reactivate a line card, MSC, or PCI port adapter carrier card in slot 2. You only need to enter this command if you enter the **hw-moduleslot** *slot-number***stop** command but do not remove the hardware and instead want to restart the hardware.

```
Router# hw-module slot 2 start
```

Related Commands

Command	Description
hw-module subslot	Prepares a SPA for online removal.
show c7300	Displays the types of cards (NSE and line cards) installed in a Cisco 7304 router.
show diag	Displays hardware information for any slot or the chassis.
show c7300 errorlog	Displays error information on a Cisco 7304 series router.
show platform errorlog	Displays error information for any installed card.

hw-module slot (7600)

To enable ports on a module, use the **hw-module slot** command in global configuration mode. To disable the ports, use the **no** form of this command.

hw-module slot *slot-number* {**memory test full** | **oversubscription** | **pos** | **process-max-time** *number-of-seconds* | **rate-limit** {**fsol_rate** *fsol-rate* | **punt_rate** *punt-packet-rate*} | **srp** | **subslot** *subslot-number* **only** | **mp-recovery-enable** | **ipv6-hbh-rl** *rate* }
no hw-module slot *slot-number* {**memory test full** | **oversubscription** | **pos** | **process-max-time** *number-of-seconds* | **rate-limit** {**fsol_rate** *fsol-rate* | **punt_rate** *punt-packet-rate*} | **srp** | **subslot** *subslot-number* **only** | **mp-recovery-enable** | **ipv6-hbh-rl** *rate* }

Syntax Description

slot-number	Chassis slot number.
memory	Specifies the memory settings of a module.
test	Specifies the memory options available for testing.
full	Performs a complete memory test on the Lower Circuit (LC).
oversubscription	Administratively disables the oversubscribed ports on a module.
pos	Converts a module to packet-over-SONET (POS) mode.
process-max-time	Specifies the maximum time for which the process runs before it stops the processor.
number-of-seconds	Number of milliseconds before the processor suspends voluntarily.
rate-limit	Limits the packets that are sent to the Route Processor (RP).
fsol_rate *fsol-rate*	Limits the broadband and Ethernet Flow Point (EFP) First Sign of Life (FSOL) packets, in bits per second (b/s). The default is 40000 b/s (or 50 packets per second for a 100-byte packet). • This keyword is specific to the ES+ line card.
punt_rate *punt-packet-rate*	Limits the Layer 4 and Port-Bundle Host Key (PBHK) packets, in bits per second (b/s). The default is 1000000 b/s. • This keyword is specific to the ES+ line card.
srp	Converts a module to Spatial Reuse Protocol (SRP) mode.
subslot *slot-number* **only**	Specifies the secondary slot number to enable a slot to support a single Shared Port Adapter (SPA).
mp-recovery-enable	Enables metropolis stuck recovery. This option is enabled by default. Use the **no** form to disable this option.

ipv6-hbh-rl *rate*	Specifies the policing rate-limit for the IPv6 Hop-by-Hop extension header packets. • For the SIP-400, you can configure a rate of up to 25600 packets per second (PPS). The default police rate is 21.36 kpps. • For the ES+ line cards, you can configure a rate of up to 100000 kbps. The default police rate is 12000 kbps.

Command Default

Ports are not enabled on a module.

Command Modes

Global configuration (config)

Command History

Release	Modification
15.1(1)S	This command was introduced.
15.2(4)S	This command was modified. The **mp-recovery-enable** keyword was added.
12.2(33)SRE6	This command was integrated into Cisco IOS Release 12.2(33)SRE6.
12.2(33)SRE7	This command was modified. The **mp-recovery-enable** keyword was added.
15.3(1)S	This command was modified. The **ipv6-hbh-rl** keyword was added.

Usage Guidelines

- The FSOL queue is used by broadband FSOL and EFP FSOL.
- The punt queue is used by Layer 4 and PBHK packets.
- An increase in the number of either FSOL or punt rate limiters enables more packets to reach the RP. This increase exerts more load on the RP CPU. Therefore, changing the default values of either FSOL or punt rate limiters is not recommended.
- On the ES+ line cards, setting the police rate to 0 turns off the policing. On the SIP-400, the policing does not stop but all the packets are dropped.
- For both the ES+ line cards and the SIP-400, when the policer is set from the line card console, the setting remains effective even if the line card is moved to another chassis running the Cisco IOS Release 15.3(1)S or later images.
- For the SIP-400, IPv6 HBH packets continue to go through the QoS policing configured on the line card. For the ES+ line cards, IPv6 HBH packets bypass any QoS policing configured on the line card.

Examples

The following example shows how to set the FSOL rate to 50000 b/s:

```
Device(config)# hw-module slot 2 rate-limit fsol_rate 50000
```

The following example shows how to set the punt rate to 70000 b/s:

```
Device(config)# hw-module slot 2 rate-limit punt_rate 70000
```

The following example shows how to set the rate limit for the IPv6 Hop-by-Hop extension header packets to 777 kbps:

```
Device(config# hw-module slot 2 ipv6-hbh-rl 777
```

Related Commands

Command	Description
show hw-module slot	Displays system information for a SPA interface processor (SIP) or a module.

hw-module slot (ASR 1000 Series)

To start, stop, reload, or enable logging for an Embedded Services Processor (ESP), Route Processor (RP), or Shared Port Adapter (SPA) Interface Processor (SIP) on a Cisco ASR 1000 Series Aggregation Services Router, use the **hw-moduleslot** command in privileged EXEC or global configuration or diagnostic mode.

hw-module slot *slot action*

Syntax Description

slot	Slot on which logging action is to be taken. Options are as follows: • *number* --the number of the SIP slot. • **f0** --The ESP in ESP slot 0. • **f1** --The ESP in ESP slot 1 • **r0** --The RP in RP slot 0. • **r1** --The RP in RP slot 1.
action	The action to take on the hardware in the specified *slot*. Options are as follows: • **logging onboard** [**disable**| **enable**] --Disables or enables onboard logging of the hardware. • **reload** --Reloads the specified hardware. • **start** --Starts the hardware if it has been stopped. • **stop** --Stops the hardware if it is currently active.

Command Default

The router sends and receives traffic by default, so this command is not necessary to enable any hardware on a router. Onboard logging for all of the hardware is enabled by default.

Command Modes

Diagnostic (diag) Privileged EXEC (#) Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Release 2.1	This command was introduced.

Usage Guidelines

The **hw-moduleslot** command does not have a **no** form.

To start, stop, or reload a SPA, use the **hw-modulesubslot**command.

The **stop** and **reload** options cannot be used on an active RP.

All traffic to hardware that has been set to stop using the **stop** option will be dropped until the hardware is reenabled by either physically removing and reinserting the hardware, or entering the **start** option. After the hardware is modified as appropriate or the **start** option is entered, the hardware has to reinitialize before it is able to send and receive traffic. Note that in some cases reinitialization can take several minutes, and that the reinitialization time required depends on the hardware and the system configuration.

When a SIP is stopped, all traffic to all SPAs in the SIP is dropped. The SPAs in the SIP can begin receiving traffic after the SIP is restarted using the **start** option and all SPAs and the SIP finish reinitializing.

Since this is a privileged EXEC-level command, this command setting cannot be saved to the startup configuration and therefore the command setting cannot be maintained after a system reload. If you want the hardware to stay in the **stop** state across system reloads, use the **hw-moduleslot***slot***shutdown** global configuration command.

The **reload** option can be used to reload hardware for any reason; for example, to finish a software upgrade that requires reloading of the hardware or to reload the hardware as part of a troubleshooting step.

The contents of onboard logging logs can be displayed using the **showloggingonboardslot** privileged EXEC and diagnostic mode commands.

Enter the **showloggingonboardslot***slot***status** privileged EXEC or diagnostic command to see if onboard logging is enabled or disabled for the hardware in a particular slot.

When the **hw-moduleslot***slot***loggingonboarddisable** command is entered, onboard logging for the specified hardware component is disabled but the existing logs are preserved; if you want to erase the existing logs, enter the **clearloggingonboardslot** command.

When the **hw-moduleslot** command is entered in global configuration mode (for ESP40 and SIP40 cards), you have a link option that allows you to choose among a set of backplane enhanced serializer/deserializer (SerDes) interconnect (ESI) links between ESP and a given SIP slot. The range of possible values for the link depends on the type of ESP and SIP cards. Only a combination of ESP40 and SIP40 cards can have more than two ESI links (link A and link B). All other cards have only link A. For example, a combination of ESP40 and SIP10 or ESP20 and SIP40 cards can have only one link (link A).

Examples

The following example shows how to stop the RP in RP slot 0:

```
Router# hw-module slot r0 stop
```

The following example shows how to disable the onboard logging for the RP in RP slot 0. The output of the **showloggingonboardslotr0status**command is given both before and after onboard logging is disabled to verify that onboard logging was properly disabled.

```
Router# show logging onboard slot r0 status

Status: Enabled
Router# hw-module slot r0 logging onboard disable
Router# show logging onboard slot r0 status

Status: Disabled
```

The following example shows how to display the available link options for ESP40 and SIP40 cards:

```
Router(config)# hw-module slot 0 qos input link ?
A  ESI Link A
B  ESI Link B
```

Related Commands

Command	Description
clear logging onboard slot	Clears the data in an onboard slot log.
hw-module subslot	Starts, stops, or reloads a SPA.

Command	Description
show logging onboard slot	Displays the status of onboard logging, or the contents of an onboard logging log.

hw-module slot image

To specify a high availability Cisco IOS image to run on an active or standby Route Switch Processor (RSP), use the **hw-moduleslotimage** command in global configuration mode. To remove a high availability Cisco IOS image from the running configuration, use the **no** form of this command.

hw-module slot *slot-number* **image** *file-spec*
no hw-module slot *slot-number* **image** *file-spec*

Syntax Description

slot-number	Specifies the number of the RSP slot.
file-spec	Specifies the flash memory card location to load the image into and the name of the image.

Command Default

No high availability Cisco IOS images are specified to run on the active or standby RSPs.

Command Modes

Global configuration

Command History

Release	Modification
12.0(16)ST	This command was introduced.
12.3(7)T	This command was integrated into Cisco IOS Release 12.3(7)T.

Examples

The following example shows a Cisco 7513 router with the active RSP loaded in slot 6 and the standby RSP loaded in slot 7. The rsp-pv-mz high availability Cisco IOS image is specified to run on both the active and the standby RSP. Both RSPs have slot 0 flash memory cards.

```
Router(config)# hw-module slot 6 image slot0:rsp-pv-mz
Router(config)# hw-module slot 7 image slot0:rsp-pv-mz
```

Related Commands

Command	Description
hw-module sec-cpu reset	Resets and reloads the standby RSP with the specified Cisco IOS image and executes the image.
mode (HSA redundancy)	Configures the redundancy mode.
redundancy	Enters redundancy configuration mode.

hw-module slot subslot only

Note This command is deleted effective with Cisco IOS Release 12.2SXI.

To change the mode of the Cisco 7600 SSC-400 card to allocate full buffers to the specified subslot, use the **hw-moduleslotsubslotonly** command in global configuration mode. If this command is not used, the total amount of buffers available is divided between the two subslots on the Cisco 7600 SSC-400.

Note This command automatically generates a reset on the Cisco 7600 SSC-400. See Usage Guidelines below for details.

hw-module slot *slot* **subslot** *subslot* **only**

Syntax Description

slot	Chassis slot number where the Cisco 7600 SSC-400 is located. Refer to the appropriate hardware manual for slot information. For SIPs and SSCs, 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.
subslot	Secondary slot number on the SSC where the IPSec VPN SPA is installed.

Command Default

No default behavior or values.

Command Modes

Global configuration mode

Command History

Release	Modification
12.2(18)SXF2	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.
12.2SXI	This command was deleted.

Usage Guidelines

Follow these guidelines and restrictions when configuring a Cisco 7600 SSC-400 and IPSec VPN SPAs using the **hw-moduleslotsubslotonly**command:

- This command is useful when supporting IP multicast over GRE on the IPSec VPN SPA.
- When this command is executed, it automatically takes a reset action on the Cisco 7600 SSC-400 and issues the following prompt to the console:

```
Module n will be reset? Confirm [n]:
```

The prompt will default to “N” (no). You must type “Y” (yes) to activate the reset action.

- When in this mode, if you manually plug in a second SPA, or if you attempt to reset the SPA (by entering a **nohw-modulesubslotshutdown** command, for example), a message is displayed on the router console which refers you to the customer documentation.

Examples

The following example allocates full buffers to the SPA that is installed in subslot 0 of the SIP located in slot 1 of the router and takes a reset action of the Cisco 7600 SSC-400.

```
Router(config)# hw-module slot 4 subslot 1 only
Module 4 will be reset? Confirm [no]: y
```

Note that the prompt will default to “N” (no). You must type “Y” (yes) to activate the reset action.

Related Commands

Command	Description
ip multicast-routing	Enables IP multicast routing.
ip pim	Enables Protocol Independent Multicast (PIM) on an interface.

hw-module standby

To reset the standby Route Processor (RP), use the **hw-modulestandby**command in privileged EXEC mode.

hw-module standby {**reset** | **reload**}

Syntax Description

reset	Resets the redundant RP.
reload	Reloads the redundant RP.

Command Default

No default behavior or values.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.1(10)EX2	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

Use this command to reset or reload the standby RP. Use the **reload** keyword to cause the standby RP to reload with an upgraded image. Use this option when the standby RP is operating normally. Use the **reset**keyword for a hard reset of the standby RP. Use this option if the standby RP is experiencing problems and does not respond to the **reload** option.

Examples

The following example shows how to reset the standby RP (NSE-100):

```
Router# hw-module standby reset
Proceed with reset of standby NSE? [confirm]y
```

The following example shows an attempt to reset a standby RP, which is down or experiencing some other problem such as being hung.

```
Router# hw-module standby reload
Proceed with reload of standby NSE? [confirm]y
%Standby RP is not up
```

If there is a failure to reset a standby RP because it is in some fault condition, try performing a reload of the RP.

The following example shows how to reload the standby RP:

```
Router# hw-module standby reload
Proceed with reload of standby NSE? [confirm]y
```

Related Commands

Command	Description
debug redundancy	Enables RP redundancy debugging.
redundancy force-switchover	Forces the standby RP to assume the role of the active RP.
show c7300	Displays the types of cards (RP and line cards) installed in a Cisco 7304 router.
show redundancy	Displays redundancy information for the active and standby RPs.

hw-module subslot

To restart, stop, or start a shared port adapter (SPA) and its interfaces, use the **hw-modulesubslot**command in privileged EXEC mode.

hw-module subslot *slot/subslot* {**reload** [**force**] | **start** | **stop** [**force**]}

For ASR 900 Series Routers, **hw-module** *slot* / *subslot* [**default** | **ether-mode 1G** | **ether-mode 10G**]

Syntax Description

slot	Physical slot number of the interface
subslot	Subslot of the interface
default	Default of all the interfaces of the interface module
ether-mode 1G	Mode of the ethernet imterface module
ether-mode 10G	Mode of the ethernet imterface module

Command Default

The SPA and its interfaces are not started.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.2(25)S3	This command was introduced.
12.2(18)SXE	This command was integrated into Cisco IOS Release 12.2(18)SXE on the Cisco 7600 series router and Catalyst 6500 series switch.
12.0(31)S	This command was integrated into Cisco IOS Release 12.0(31)S.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
Cisco IOS XE Release 2.4	This commad was modified. The **force** keyword was added. This command was integrated into Cisco IOS XE Release 2.4.
Cisco IOS XE 16.5.1 Everest	The keyword **ether-mode 1G** was introduced.

Usage Guidelines

The **hw-modulesubslot** command stops and starts power to the SPA. This command is useful when you want to restart all interfaces on a SPA. When the **stop** and **reload** keywords are used, you get a prompt to confirm. Enter “y” or use the return key to confirm. Power to the SPA is now stopped or reloaded. If you use the **force** keyword along with the **reload** keyword, you can proceed further without getting any prompt for confirmation. The Excalibur and Ethernet Services cards do not have the **reload** option.

The command is recommended to restart a SPA under the following conditions:

- To restart a SPA after it has been powered off because of a failure.
- To recover from corrupted messaging between the Route Processor (RP) and the SIP.

Examples

The following command power cycles the SPA in subslot 1 of the SIP installed in chassis slot 1:

```
Router# hw-module subslot 1/1 reload
Proceed with reload of module? [confirm]
```

Related Commands

Command	Description
show hw-module subslot oir	Displays the operational status of a SPA.

hw-module subslot (4400)

To restart, stop, or start a module and its interfaces, use the **hw-modulesubslot** command in privileged EXEC mode.

hw-module subslot *slot/subslot* {**reload** | **start** | **stop** }

Syntax Description

reload	Restarts the target subslot.
slot	Specifies the chassis slot number where the module is installed. Refer to the hardware installationg guide for more information on slots. For module and interfaces, refer to the module-specific hardware installation guide.
start	Activates the specified module.
stop	Stops the specified module.
/ *subslot*	Specifies the subslot number of the chassis where the module is installed. Refer to the hardware installation guide for subslot information.

Command Default

The modules and its interfaces are not activated.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Release 3.9S	This command was introduced.

Usage Guidelines

The **hw-module subslot** command allows you to stop and start the power supply to a supported cisco services or network interface module (NIM) on a Cisco 4400 Series Integrated Services Router (ISR). This functionality is also referred as the online insertion and removal (OIR) and it is useful when you want to remove a module from one of the subslots while another active module remains installed on your router.

Note If you are not planning to immediately replace a module, ensure that you install a blank filter plate in the subslot.

The **stop** option allows you to gracefully deactivate a module and the module is rebooted when the **start** command is executed. The **reload** option will stop or deactivate a specified module and restart it.

Examples

The following command activates a module in subslot 1:

```
Router# hw-module subslot 1/1 start
```

Related Commands

Command	Description
show hw-module subslot oir	Displays the operational status of a module.

hw-module subslot ethernet vlan unlimited

To remove the restriction of a maximum of 8100 IEEE 802.1Q VLANs per Ethernet shared port adapter (SPA), use the **hw-modulesubslotethernetvlanunlimited** command in global configuration mode. To disable and return to a maximum limit of 8100 VLANs per SPA, use the **no** form of this command.

hw-module subslot *slot/subslot* **ethernet vlan unlimited**
no hw-module subslot *slot/subslot* **ethernet vlan unlimited**

Syntax Description

slot /	Specifies the chassis slot number where the SIP is installed.
subslot	Specifies the slot of the SIP where the SPA is installed.

Command Default

There is no default behavior or values. When this command is not configured, up to 8100 dot1q VLANs per Ethernet SPA are supported.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Release 2.5	This command was introduced.

Usage Guidelines

For any Ethernet SPA on the Cisco ASR 1000 Series aggregation services routers, the maximum number of IEEE 802.1Q VLANs that can be configured per port is 4094. The default total maximum number of VLANs per SPA is 8100.

The limit on this total maximum number of VLANs per SPA (which means, the default of 8100 VLANs) can be removed using the **hw-modulesubslotethernetvlanunlimited** command. However, the limit on the maximum number of VLANs per Ethernet port or interface (i.e. 4094) still applies. Therefore, the new maximum number of supported VLANs per SPA varies by the number of ports on the SPA multiplied by 4094. On the 5-Port Gigabit Ethernet SPA, you can configure up to 20,470 dot1q (or unambiguous QinQ) VLANs. On an 8-Port Gigabit Ethernet SPA, you can configure up to 32752 dot1q (or unambiguous QinQ) VLANs.

When the **hw-modulesubslotethernetvlanunlimited** command is configured, VLAN filtering, accounting, and classification are no longer performed by the Ethernet SPA and all 802.1Q frames and QinQ frames are processed by the Quantum Flow Processor (QFP) on the Cisco ASR1000 Series Router. Sending all of the dot1q VLAN frames to the QFP (without filtering) may reduce the QFP packet switching performance.

The default classification of CoS bits 6-7 as high priority is still supported. However, other user-defined CoS values for high and low priority classification using the **plimqosinputmapcosqueue** command are not supported when this command is in use.

Examples

The following example enables support for maximum per-port dot1q VLAN configuration for the SPA located in the first subslot (0) of the SIP located in slot 1 of the Cisco ASR1000 Series Router:

```
Router(config)# hw-module subslot 1/0 ethernet vlan unlimited
```

Related Commands

Command	Description
show interfaces	Displays statistics for all interfaces configured on the router.

hw-module subslot (LAN WAN)

To configure the Cisco 1-Port 10 Gigabit Ethernet LAN/WAN-PHY Shared Port Adapter to run in either the LAN mode or WAN mode, use the **hw-modulesubslotslot/subslotenable{LAN|WAN}**commandin Global configuration mode.

hw-module subslot *slot/subslot* **enable** {**LAN** | **WAN**}

Syntax Description

slot/subslot	The slot and subslot number in which the Cisco 1-Port 10 Gigabit Ethernet LAN/WAN-PHY Shared Port Adapter has been installed.
enable	Enables the specified LAN or WAN operational mode on the SPA.
LAN	Specifies the LAN mode of operation for theCisco 1-Port 10 Gigabit Ethernet LAN/WAN-PHY Shared Port Adapter.
WAN	Specifies the WAN mode of operation for the Cisco 1-Port 10 Gigabit Ethernet LAN/WAN-PHY Shared Port Adapter.

Command Default

By default, the Cisco 1-Port 10 Gigabit Ethernet LAN/WAN-PHY Shared Port Adapter operates in the WAN mode when the SPA boots-up.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Release 3.3.0S	This command was introduced on the Cisco ASR 1000 Series Routers.

Usage Guidelines

By default, the Cisco 1-Port 10 Gigabit Ethernet LAN/WAN-PHY Shared Port Adapter initializes in the WAN mode. The Cisco 1-Port 10 Gigabit Ethernet LAN/WAN-PHY Shared Port Adapter can operate in either the LAN mode or the WAN mode. To change the LAN mode or WAN mode, execute the **hw-modulesubslot***slot/subslot***enable** {**LAN** | **WAN**} command from the Global configuration mode.

Examples

The following example shows how to enable the LAN mode on a Cisco 1-Port 10 Gigabit Ethernet LAN/WAN-PHY Shared Port Adapter:

```
Router# config
Router(config)# hw-module subslot 2/1 enable LAN
```

The following example shows how to enable the WAN mode on a Cisco 1-Port 10 Gigabit Ethernet LAN/WAN-PHY Shared Port Adapter:

```
Router# config
Router(config)# hw-module subslot 2/1 enable WAN
```

Tip If the Cisco 1-Port 10 Gigabit Ethernet LAN/WAN-PHY Shared Port Adapter is working in LAN mode, you can change the mode to WAN by either using the **hw-modulesusblot***slot/subslot***enableWAN** command.

Related Commands

Command	Description
show controllers wanphy	Displays the SPA mode (LAN mode or WAN mode), alarms, and the J1 byte string value.

hw-module subslot service-engine session

To open a console session to access the Cisco WebEx Node SPA console, use the **hw-modulesubslotservice-enginesession**command in privileged EXEC mode.

hw-module subslot *slot*/*subslot* **service-engine session**

Syntax Description

slot	Specifies the chassis slot number for the Cisco ASR 1000 Series Router SIP.
/ *subslot*	Specifies the secondary subslot number on a Cisco ASR 1000 Series Router SIP where a SPA is installed.

Command Default

No command default.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
IOS XE Release 2.4	This command was introduced.

Usage Guidelines

To open a console session on a Cisco WebEx Node SPA, the SPA must first be configured with a minimum of the following commands:

- **ip address**
- **service-engine ip address**
- **service-engine default-gateway**

The **service-engineipaddress** command must be configured before the **service-enginedefault-gateway** command.

Examples

The following example shows how to access the console for a WebEx Node SPA located in slot 1/0, and the change to the SPA console prompt (service-spa is the default hostname) when complete:

```
Router# hw-module subslot 1/0 service-engine session
MontaVista(R) Linux(R) Carrier Grade Edition 5.0 (custom)
Linux/mips64 2.6.21_mvlcge500-octeon-mips64_octeon_v2_be
        Vegas Shell  --  CGE 5.0 Version
        Copyright (c) 1985-2008 by Cisco Systems, Inc.
        All rights reserved.
service-spa#
```

Related Commands

Command	Description
service-engine default-gateway	Defines a default gateway router IP address for the Cisco WebEx Node SPA.

Command	Description
service-engine ip address	Selects and configures the internal interface for management traffic on a Cisco WebEx Node SPA.

hw-module subslot session

To start or close a Cisco Integrated Management Controller (CIMC) session or host server module session, use the **hw-module subslot session** command in privileged EXEC mode.

hw-module subslot *slot/subslot* **session** {**imc** | **server**}

Syntax Description

slot/	Number of the router slot in which the server module is installed. **Note** For the NIM E-Series NCE, the slot number is 0.
subslot	Number of the subslot in which the server module is installed. **Note** For Cisco UCS E-Series Servers and the SM E-Series NCE, the subslot number is 0.
imc	Starts a session with CIMC.
server	Starts a session with the host server module.

Command Modes

Privileged EXEC (#)

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).
Cisco IOS XE Release 3.15S	This command was supported on an additional platform: the NIM E-Series Network Compute Engine (NIM E-Series NCE) installed in a Cisco ISR 4000 series.

Usage Guidelines

Only one active session is allowed on the CIMC or server module at any time.

Examples

The following example shows how to start a CIMC session in an E-Series Server installed in a Cisco ISR 4000 series:

```
Router# hardware-module subslot 1/0 session imc
```

The following example shows how to start a server module session in an E-Series Server installed in a Cisco ISR 4000 series:

```
Router# hardware-module subslot 1/0 session server
```

hw-module subslot shutdown

To disable a shared port adapter (SPA) with or without power, and save the configuration to the configuration file, use the **hw-modulesubslotshutdown**command in global configuration mode. To re-enable the SPA, use the **no** form of this command.

hw-module subslot *slot/subslot* **shutdown** [**powered** | **unpowered**]
no hw-module subslot *slot/subslot* **shutdown** [**powered** | **unpowered**]

Syntax Description

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.
/ *subslot*	Secondary slot number on a SPA interface processor (SIP) where a SPA is installed. 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.
powered	(Optional) Shuts down the SPA and all of its interfaces, and leaves them in an administratively down state with power enabled. This is the default state.
unpowered	(Optional) Shuts down the SPA and all of its interfaces, and leaves them in an administratively down state wihout power.

Command Default

If this command is not used, **nohw-modulesubslotshutdown** is the default behavior. When **nohw-modulesubslot** is configured, the SPA will be powered for normal operation.

If the **hw-modulesubslotshutdown** command is entered but neither **powered** or **unpowered** are specified in the CLI, **powered** is the default behavior.

Command Modes

Global configuration

Command History

Release	Modification
12.2(25)S3	This command was introduced.
12.2(18)SXE	This command was integrated into Cisco IOS Release 12.2(18)SXE.
12.0(31)S	This command was integrated into Cisco IOS Release 12.0(31)S.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

When you shut down a SPA using this command, you can choose to put it into one of two states:

- Powered state--(Default) Shuts down the SPA, but the SPA remains powered on. Use this option when you plan to leave the SPA physically installed and cabled in the SPA. You might choose to do this if you

want to install a SPA and configure it, but do not want it online or to start communicating with the remote end of the connection.

- Unpowered state--Shuts down the SPA and removes power from the SPA. Use this option when you plan to remove the SPA from the chassis.

This command is useful when a user wants all the interfaces on a SPA disabled but does not or cannot remove the SPA. Unlike the **hw-modulesubslotstop** EXEC command on the Cisco 7304 router, this command is saved in the configuration file and will keep the SPA disabled when other router events (such as a router reload or OIR) attempt to restart the SPA. All other settings and configurations of the SPA will be maintained even if the SPA itself is shutdown using this command.

As a general rule, you do not need to shut down a SPA if you are removing it and replacing it with the same exact model of SPA in an online insertion and removal (OIR) operation. However, you should shut down a SPA whenever you are replacing a SPA with a different model of SPA.

When you shut down a SPA using the **hw-modulesubslotshutdown**command, it remains shutdown even if you reset the SPA or install a new SPA in that subslot. To begin using the card again, you must manually re-enable the card using the **nohw-modulesubslotshutdown**command.

Note This is a global configuration command, not an EXEC command. On the Cisco 7304 router, another **hw-modulesubslot** command is also available in EXEC mode, but that command is used for different purposes. An important distinction between this command and the **hw-modulesubslot** command in EXEC mode on the Cisco 7304 router is that this command is saved in the configuration.

Examples

The following example shows how to disable the SPA in subslot 4/1 while leaving the SPA in the SPA chassis. This command will be saved to the configuration file and no actions, outside of changing this configuration, will re-enable the SPA:

```
Router(config)# hw-module subslot 4/1 shutdown unpowered
```

The following example shows how to configure the SPA to resume normal operation after the unpowered option has been used to disable the SPA:

```
Router(config)# hw-module subslot 4/1 shutdown powered
```

No messages are provided on the console when you shut down or re-enable a SPA.

Related Commands

Command	Description
show hw-module subslot oir	Displays the operational status of a SPA.
hw-module slot [1]	Deactivates or reactivates a carrier card that is installed in a router slot. This command is entered in EXEC mode and is not saved to the configuration file.

[1] Refer to the Cisco 7300 Series Platform-Specific Commands publication.

hw-module subslot shutdown (4400)

To disable a module with or without power, and save the configuration to the configuration file, use the **hw-module subslot shutdown** command in global configuration mode. To re-activate the module, use the **no** form of this command.

hw-module subslot *slot / subslot* **shutdown** [**powered** | **unpowered**]
no hw-module subslot *slot / subslot* **shutdown** [**powered** | **unpowered**]

Syntax Description

slot	Specifies the chassis slot number where the module installed. Refer to the hardware installation guide for more information on slots. For information on modules and interfaces, refer to the module specific hardware installation guide.
/ *subslot*	Specifies the subslot number of the chassis where the module is installed. Refer to the hardware installation guide for subslot information.
powered	(Optional) Shuts down the module and all of its interfaces, and leaves them in an administratively down state with power enabled. This is the default state.
unpowered	(Optional) Shuts down the module and all of its interfaces, and leaves them in an administratively down state without power.

Command Default

If this command is not used, **no hw-module subslot shutdown** is the default behavior. When **no hw-module subslot** is configured, the module is powered on for normal operation.

If the **hw-module subslot shutdown** command is entered but neither **powered** or **unpowered** are specified in the CLI, **powered** is the default behavior.

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS XE Release 3.9S	This command was introduced.

Usage Guidelines

When you shut down a Cisco Services or Network Interface Module (NIM) using this command, you can choose to put it into one of two states:

- Powered state--(Default) Shuts down the module, but the router remains powered on. Use this option when you plan to leave the module physically installed and cabled into the router. You might choose to do this if you want to install a module and configure it, but do not want it online or to start communicating with the remote end of the connection.
- Unpowered state--Shuts down the module and removes power from the module. Use this option when you plan to remove the module from the chassis.

If you choose to deactivate your module and its interfaces by executing the **hw-module subslot shutdown** command in global configuration mode, you are able to change the configuration in such a way that no matter how many times the router is rebooted, the module does not boot. This command is useful when you need to shut down a module located in a remote location and ensure that it does not boot automatically when the router

is rebooted. To begin using the interface again, you must manually re-enable the module using the **no hw-module subslot shutdown** command.

Examples

The following example shows how to disable the module in subslot 0/2 without removing the module from the router :

```
Router(config)# hw-module subslot 0/2 shutdown unpowered
```

The following example shows how to configure a module to resume normal operation after the unpowered option has been used to disable the module:

```
Router(config)# hw-module subslot 0/2 shutdown powered
```

Related Commands

Command	Description
show hw-module subslot oir	Displays the operational status of a module.
hw-module subslot	Deactivates or reactivates a module in a router slot. This command is entered in EXEC mode and is not saved to the configuration file.