



Interface Commands

This book describes the basic commands that can be used on different types of interfaces. These commands correspond to the interface configuration tasks included in the Cisco IOS configuration guides. Refer to the configuration guide indicated here for configuration guidelines:

For information about this type of interface . . .	Refer to this publication . . .
General interface	“Interface Configuration Overview” chapter in the <i>Cisco IOS Interface Configuration Guide</i>
LAN interface	“Configuring LAN Interfaces” chapter in the <i>Cisco IOS Interface Configuration Guide</i>
Serial interface	“Configuring Serial Interfaces” chapter in the <i>Cisco IOS Interface Configuration Guide</i>
Logical interface	“Configuring Logical Interfaces” chapter in the <i>Cisco IOS Interface Configuration Guide</i>
Cisco Mainframe Channel Connection (CMCC) adapters	“Configuring Cisco Mainframe Channel Connection Adapters” chapter in the <i>Cisco IOS Bridging and IBM Networking Configuration Guide</i>
Dialer interface and virtual-access interface	<i>Cisco IOS Dial Technologies Configuration Guide and Cisco IOS Dial Technologies Command Reference</i>
ISDN PRI interface	<i>Cisco IOS Dial Technologies Configuration Guide and Cisco IOS Dial Technologies Command Reference</i>

Other interface commands, specific to a particular technology area, are described in the technology specific configuration guides. For example, for hardware technical descriptions, and for information about installing the router or access server interfaces, refer to the hardware installation and maintenance publication for your particular product.

The LAN Extension feature will no longer be offered after Cisco IOS Release 12.2(15)T. LAN Extension documentation in the *Cisco IOS Interface Command Reference*, Release 12.2 can be accessed at:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/finter_r/index.htm

The following LAN Extension commands have been removed from documentation in Cisco IOS Software Release 12.2(15)T and will not appear in future releases of the Cisco IOS software documentation set:

- clear controller lex
- copy flash lex
- copy tftp lex
- lex burned-in-address
- lex input-address-list
- lex input-type-list
- lex priority group
- lex retry-count
- lex timeout
- show controllers lex
- show interfaces lex

alarm-interface

To enter alarm interface mode and configure the alarm interface controller (AIC), use the **alarm-interface** command in global configuration mode. To leave alarm interface mode, use the **exit** command.

alarm-interface *slot-number*

Syntax Description	<i>slot-number</i>	Number of the port in which the AIC is installed.
--------------------	--------------------	---

Defaults	No default behavior or values
----------	-------------------------------

Command Modes	Global configuration
---------------	----------------------

Command History	Release	Modification
	12.2(2)XG	This command was introduced for the Cisco 2600 series and the Cisco 3600 series.
	12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T.

Examples The following examples show how the **alarm-interface** command is used in conjunction with the **ip address** and the **reset** commands:

```
Router(config)# alarm-interface 5
Router(config-aic)# ip address 10.2.130.105
```

A change in the AIC IP configuration might not take effect until the next time the card is started. Use the **reset** command to restart the card, as in the following example:

```
Router(config-aic)# reset
Alarm Interface Card in slot 5 restarted

Router(config-aic)# end
```

Related Commands	Command	Description
	ip address	Sets a primary or secondary IP address for an interface.
	reset	Resets the AIC CPU.

aps authenticate

To enable authentication and specify the string that must be present to accept any packet on the out-of-band (OOB) communications channel on a packet-over-SONET (POS) interface, use the **aps authenticate** command in interface configuration mode. To disable authentication, use the **no** form of this command.

aps authenticate *string*

no aps authenticate

Syntax Description	<i>string</i>	Text that must be present to accept the packet on a protected or working interface. A maximum of eight alphanumeric characters are accepted.
---------------------------	---------------	--

Defaults Authentication is disabled.

Command Modes Interface configuration

Command History	Release	Modification
	11.1 CC	This command was introduced.

Usage Guidelines Use the **aps authenticate** command to ensure that only valid packets are accepted on the OOB communications channel.

The **aps authenticate** command must be configured on both the working and protect interfaces.

Examples The following example enables authentication on POS interface 0 in slot 4:

```
Router# configure terminal
Router(config)# interface pos 4/0/0
Router(config-if)# aps working 1
Router(config-if)# aps authenticate sanjose
Router(config-if)# exit
Router(config)# exit
Router#
```

Related Commands	Command	Description
	aps protect	Enables a POS interface as a protect interface.
	aps working	Configures a POS interface as a working interface.

aps force

To manually switch the specified circuit to a protect interface, unless a request of equal or higher priority is in effect, use the **aps force** command in interface configuration mode. To cancel the switch, use the **no** form of this command.

aps force *circuit-number*

no aps force *circuit-number*

Syntax Description

<i>circuit-number</i>	Number of the circuit to switch to the protect interface.
-----------------------	---

Defaults

No circuit is switched.

Command Modes

Interface configuration

Command History

Release	Modification
11.1 CC	This command was introduced.

Usage Guidelines

Use the **aps force** command to manually switch the interface to a protect interface when you are not using the **aps revert** command. For example, if you need to change the fiber connection, you can manually force the working interface to switch to the protect interface.

In a one-plus-one (1+1) configuration only, you can use the **aps force 0** command to force traffic from the protect interface back onto the working interface.

The **aps force** command has a higher priority than any of the signal failures or the **aps manual** command.

The **aps force** command is configured only on protect interfaces.

Examples

The following example forces the circuit on POS interface 0 in slot 3 (a protect interface) back onto a working interface:

```
Router# configure terminal
Router(config)# interface pos 3/0/0
Router(config-if)# aps protect 10/30/1/1
Router(config-if)# aps force 1
Router(config-if)# exit
Router(config)# exit
```

Related Commands	Command	Description
	aps manual	Manually switches a circuit to a protect interface.
	aps protect	Enables a POS interface as a protect interface.
	aps working	Configures a POS interface as a working interface.

aps group

To allow more than one protect and working interface to be supported on a router, use the **aps group** command in interface configuration mode. To remove a group, use the **no** form of this command.

aps group *group-number*

no aps group *group-number*

Syntax Description

<i>group-number</i>	Number of the group.
---------------------	----------------------

Defaults

No groups exist.



Note

0 is a valid group number.
The default *group-number* is 0.
The **aps group 0** command does not imply that no groups exist.

Command Modes

Interface configuration

Command History

Release	Modification
11.1 CC	This command was introduced.

Usage Guidelines

Use the **aps group** command to specify more than one working and protect interfaces on a router, for example, working channel for group 0 and protect channel for group 1 on one router, and working channel for group 1 and protect channel for group 0 on another router.

The **aps group** command must be configured on both the protect and working interfaces.

Examples

The following example configures two working/protect interface pairs. Working interface (3/0/0) is configured in group 10 (the protect interface for this working interface is configured on another router), and protect interface (2/0/1) is configured in group 20:

```
Router# configure terminal
Router(config)# interface ethernet 0/0
Router(config-if)# ip address 10.7.7.6 255.255.255.0
Router(config-if)# exit
Router(config)# interface pos 3/0/0
Router(config-if)# aps group 10
Router(config-if)# aps working 1
Router(config-if)# exit
Router(config)# interface pos 2/0/1
Router(config-if)# aps group 20
Router(config-if)# aps protect 1 10.7.7.7
Router(config-if)# end
```

On the second router, protect interface (4/0/0) is configured in group 10, and working interface (5/0/0) is configured in group 20 (the protect interface for this working interface is configured on another router):

```
Router(config)# interface ethernet 0/0
Router(config-if)# ip address 7.7.7.7 255.255.255.0
Router(config-if)# exit
Router(config)# interface pos 4/0/0
Router(config-if)# aps group 10
Router(config-if)# aps protect 1 7.7.7.6
Router(config-if)# exit
Router(config)# interface pos 5/0/0
Router(config-if)# aps group 20
Router(config-if)# aps working 1
Router(config-if)# exit
Router(config)# end
Router#
```

Related Commands

Command	Description
aps protect	Enables a POS interface as a protect interface.
aps working	Configures a POS interface as a working interface.

aps lockout

To prevent a working interface from switching to a protect interface, use the **aps lockout** command in interface configuration mode. To remove the lockout, use the **no** form of this command.

aps lockout *circuit-number*

no aps lockout *circuit-number*

Syntax Description	<i>circuit-number</i>	Number of the circuit to lock out.
--------------------	-----------------------	------------------------------------

Defaults	No lockout exists.
----------	--------------------

Command Modes	Interface configuration
---------------	-------------------------

Command History	Release	Modification
	11.1 CC	This command was introduced.

Usage Guidelines	The aps lockout command is configured only on protect interfaces.
------------------	--

Examples	This example locks out POS interface 3/0/0 (that is, prevents the circuit from switching to a protect interface in the event that the working circuit becomes unavailable):
----------	---

```
Router# configure terminal
Router(config)# interface pos 3/0/0
Router(config-if)# aps protect 1 10.7.7.7
Router(config-if)# aps lockout 1
Router(config-if)# end
Router#
```

Related Commands	Command	Description
	aps protect	Enables a POS interface as a protect interface.
	aps working	Configures a POS interface as a working interface.

aps manual

To manually switch a circuit to a protect interface, use the **aps manual** command in interface configuration mode. To cancel the switch, use the **no** form of this command.

aps manual *circuit-number*

no aps manual *circuit-number*

Syntax Description	<i>circuit-number</i>	Number of the circuit to switch to a protect interface.
---------------------------	-----------------------	---

Defaults	No circuit is switched.
-----------------	-------------------------

Command Modes	Interface configuration
----------------------	-------------------------

Command History	Release	Modification
	11.1 CC	This command was introduced.

Usage Guidelines

Use the **aps manual** command to manually switch the interface to a protect interface. For example, you can use this feature when you need to perform maintenance on the working channel. If a protection switch is already up, you can also use the **aps manual** command to revert the communication link back to the working interface before the wait to restore (WTR) time has expired. The WTR time period is set by the **aps revert** command.

In a one-plus-one (1+1) configuration only, you can use the **aps manual 0** command to force traffic from the protect interface back onto the working interface.

The **aps manual** command is a lower priority than any of the signal failures or the **aps force** command.

Examples

The following example forces the circuit on POS interface 0 in slot 3 (a working interface) back onto the protect interface:

```
Router# configure terminal
Router(config)# interface pos 3/0/0
Router(config-if)# aps working 1
Router(config-if)# aps manual 1
Router(config-if)# end
Router#
```

Related Commands	Command	Description
	aps force	Manually switches the specified circuit to a protect interface, unless a request of equal or higher priority is in effect.
	aps protect	Enables a POS interface as a protect interface.

Command	Description
aps revert	Enables automatic switchover from the protect interface to the working interface after the working interface becomes available.
aps working	Configures a POS interface as a working interface.

aps protect

To enable a POS interface as a protect interface, use the **aps protect** command in interface configuration mode. To remove the POS interface as a protect interface, use the **no** form of this command.

aps protect *circuit-number ip-address*

no aps protect *circuit-number ip-address*

Syntax Description	
<i>circuit-number</i>	Number of the circuit to enable as a protect interface.
<i>ip-address</i>	IP address of the router that has the working POS interface.

Defaults No circuit is protected.

Command Modes Interface configuration

Command History	Release	Modification
	11.1 CC	This command was introduced.

Usage Guidelines Use the **aps protect** command to configure the POS interface used by a working interface if the working interface becomes unavailable because of a router failure, degradation or loss of channel signal, or manual intervention.



Caution

Configure the working interface before configuring the protect interface to keep the protect interface from becoming the active circuit and disabling the working circuit when it is finally discovered.

Examples The following example configures circuit 1 on POS interface 5/0/0 as a protect interface for the working interface on the router with the IP address of 10.7.7.7. For information on how to configure the working interface, refer to the **aps working** command.

```
Router# configure terminal
Router(config)# interface pos 5/0/0
Router(config-if)# aps protect 1 10.7.7.7
Router(config-if)# end
Router#
```

Related Commands	Command	Description
	aps working	Configures a POS interface as a working interface.

aps revert

To enable automatic switchover from the protect interface to the working interface after the working interface becomes available, use the **aps revert** command in interface configuration mode. To disable automatic switchover, use the **no** form of this command.

aps revert *minutes*

no aps revert

Syntax Description	<i>minutes</i>	Number of minutes until the circuit is switched back to the working interface after the working interface is available.
---------------------------	----------------	---

Defaults Automatic switchover is disabled.

Command Modes Interface configuration

Command History	Release	Modification
	11.1 CC	This command was introduced.

Usage Guidelines Use the **aps revert** command to return the circuit to the working interface when it becomes available. The **aps revert** command is configured only on protect interfaces.

Examples The following example enables circuit 1 on POS interface 5/0/0 to revert to the working interface after the working interface has been available for 3 minutes:

```
Router# configure terminal
Router(config)# interface pos 5/0/0
Router(config-if)# aps protect 1 10.7.7.7
Router(config-if)# aps revert 3
Router(config-if)# end
Router#
```

Related Commands	Command	Description
	aps protect	Enables a POS interface as a protect interface.

aps timers

To change the time between hello packets and the time before the protect interface process declares a working interface router to be down, use the **aps timers** command in interface configuration mode. To return to the default timers, use the **no** form of this command.

```
aps timers seconds1 seconds2
```

```
no aps timers
```

Syntax Description	
<i>seconds1</i>	Number of seconds to wait before sending a hello packet (hello timer).
<i>seconds2</i>	Number of seconds to wait to receive a response from a hello packet before the interface is declared down (hold timer).

Defaults Hello time is 1 second, and hold time is 3 seconds.

Command Modes Interface configuration

Command History	Release	Modification
	11.1 CC	This command was introduced.

Usage Guidelines Use the **aps timers** command to control the time between an automatic switchover from the protect interface to the working interface after the working interface becomes available.

Normally, the hold time is greater than or equal to three times the hello time.

The **aps timers** command is configured only on protect interfaces.

Examples The following example specifies a hello time of 2 seconds and a hold time of 6 seconds on circuit 1 on POS interface 5/0/0:

```
Router# configure terminal
Router(config)# interface pos 5/0/0
Router(config-if)# aps working 1
Router(config-if)# aps timers 2 6
Router(config-if)# end
Router#
```

aps unidirectional

To configure a protect interface for unidirectional mode, use the **aps unidirectional** command in interface configuration mode. To return to the default, bidirectional mode, use the **no** form of this command.

aps unidirectional

no aps unidirectional

Syntax Description

This command has no arguments or keywords.

Defaults

Bidirectional mode

Command Modes

Interface configuration

Command History

Release	Modification
11.1 CC	This command was introduced.

Usage Guidelines

Use the **aps unidirectional** command when you must interoperate with SONET network equipment, Add Drop Multiplexor(s) (ADMs) that supports unidirectional mode.



Note

We recommend bidirectional mode when it is supported by the interconnecting SONET equipment. When the protect interface is configured as unidirectional, the working and protect interfaces must cooperate to switch the transmit and receive SONET channel in a bidirectional fashion. This happens automatically when the SONET network equipment is in bidirectional mode.

The **aps unidirectional** command is configured only on protect interfaces.

Examples

The following example configures POS interface 3/0/0 for unidirectional mode:

```
Router# configure terminal
Router(config)# interface pos 3/0/0
Router(config-if)# aps unidirectional
Router(config-if)# aps protect 1 7.7.7.7
Router(config-if)# end
Router#
```

aps working

To configure a Packet over SONET (POS) interface as a working interface, use the **aps working** command in interface configuration mode. To remove the protect option from the POS interface, use the **no** form of this command.

aps working *circuit-number*

no aps working *circuit-number*

Syntax Description

circuit-number Circuit number associated with this working interface.

Defaults

No circuit is configured as working.

Command Modes

Interface configuration

Command History

Release	Modification
11.1 CC	This command was introduced.

Usage Guidelines

When a working interface becomes unavailable because of a router failure, degradation or loss of channel signal, or manual intervention, the circuit is switched to the protect interface to maintain the connection.

To enable the circuit on the protect interface to switch back to the working interface after the working interface becomes available again, use the **aps revert** command in interface configuration mode.



Caution

Configure the working interface before configuring the protect interface to keep the protect interface from becoming the active circuit and disabling the working circuit when it is finally discovered.

Examples

The following example configures POS interface 0 in slot 4 as a working interface. For information on how to configure the protect interface, refer to the **aps protect** command.

```
Router# configure terminal
Router(config)# interface pos 4/0/0
Router(config-if)# aps working 1
Router(config-if)# end
Router#
```

Related Commands

Command	Description
aps protect	Enables a POS interface as a protect interface.
aps revert	Enables automatic switchover from the protect interface to the working interface after the working interface becomes available.

atm sonet

To set the mode of operation and thus control the type of the ATM cell used for cell-rate decoupling on the SONET physical layer interface module (PLIM), use the **atm sonet** command in interface configuration mode. To restore the default Synchronous Transport Signal level 12, concatenated (STS-12c) operation, use the **no** form of this command.

atm sonet [stm-4]

no atm sonet [stm-4]

Syntax Description	stm-4	(Optional) Synchronous Digital Hierarchy/Synchronous Transport Signal level 4 (SDH/STM-4) operation (ITU-T specification).
---------------------------	--------------	--

Defaults	STS-12c
-----------------	---------

Command Modes	Interface configuration
----------------------	-------------------------

Command History	Release	Modification
	11.1 CC	This command was introduced.
	11.2 GS	The stm-4 keyword was added.

Usage Guidelines	Use STM-4 in applications in which SDH framing is required. Use the default (STS-12c) in applications in which the ATM switch requires “unassigned cells” for rate adaptation. An unassigned cell contains 32 zeros.
-------------------------	---

Examples	The following example sets the mode of operation to SONET STM-4 on ATM interface 3/0:
-----------------	---

```
Router(config)# interface atm 3/0
Router(config-if)# atm sonet stm-4
Router(config-if)# end
Router#
```

auto-polarity

To enable automatic receiver polarity reversal on a hub port connected to an Ethernet interface of a Cisco 2505 or Cisco 2507 router, use the **auto-polarity** command in hub configuration mode. To disable this feature, use the **no** form of this command.

auto-polarity

no auto-polarity

Syntax Description This command has no arguments or keywords.

Defaults Enabled

Command Modes Hub configuration

Command History	Release	Modification
	10.3	This command was introduced.

Usage Guidelines This command applies to a port on an Ethernet hub only.

Examples The following example enables automatic receiver polarity reversal on hub 0, ports 1 through 3:

```
Router(config)# hub ethernet 0 1 3
Router(config-hub)# auto-polarity
```

Related Commands	Command	Description
	hub	Enables and configures a port on an Ethernet hub of a Cisco 2505 or Cisco 2507 router.

bandwidth (interface)

To set and communicate the current bandwidth value for an interface to higher-level protocols, use the **bandwidth** command in interface configuration mode. To restore the default values, use the **no** form of this command.

bandwidth *kilobits*

no bandwidth

Syntax Description

<i>kilobits</i>	Intended bandwidth, in kilobits per second. For a full bandwidth DS3, enter the value 44736.
-----------------	--

Defaults

Default bandwidth values are set during startup; the bandwidth values can be displayed using the **show interface EXEC** command.

Command Modes

Interface configuration

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines

Bandwidth Information

The **bandwidth** command sets an informational parameter to communicate only the current bandwidth to the higher-level protocols; you cannot adjust the actual bandwidth of an interface with this command.



Note

This is a routing parameter only; it does not affect the physical interface.

Changing Bandwidth

For some media, such as Ethernet, the bandwidth is fixed; for other media, such as serial lines, you can change the actual bandwidth by adjusting hardware. For both classes of media, you can use the **bandwidth** configuration command to communicate the current bandwidth to the higher-level protocols.

Examples

The following example sets the full bandwidth for DS3 transmissions:

```
Router(config)# interface serial 0
Router(config-if)# bandwidth 44736
```

Related Commands

Command	Description
show interfaces	Displays statistics for all interfaces configured on the router.

carrier-delay

To set the carrier delay on a serial interface, use the **carrier-delay** command in interface configuration mode. To return to the default carrier delay value, use the **no** form of this command.

carrier-delay [*seconds* | **msec** *milliseconds*]

no carrier-delay [*seconds* | **msec** *milliseconds*]

Syntax Description	
<i>seconds</i>	(Optional) Time, in seconds, to wait for the system to change states. The range is from 0 to 60. The default is 2.
msec <i>milliseconds</i>	(Optional) Time in milliseconds. The default is 50 milliseconds.

Defaults The default carrier delay is 2 seconds; the default in milliseconds is 50 milliseconds.

Command Modes Interface configuration

Command History	Release	Modification
	10.1	This command was introduced.

Usage Guidelines If a link goes down and comes back up before the carrier delay timer expires, the down state is effectively filtered, and the rest of the software on the switch is not aware that a link-down event occurred. Therefore, a large carrier delay timer results in fewer link-up/link-down events being detected. On the other hand, setting the carrier delay time to 0 means that *every* link-up/link-down event is detected.

In most environments a lower carrier delay is better than a higher one. The exact value that you choose depends on the nature of the link outages that you expect to see in your network and how long you expect those outages to last.

If data links in your network are subject to short outages, especially if those outages last less than the time it takes for your IP routing to converge, you should set a relatively long carrier delay value to prevent these short outages from causing unnecessary churn in your routing tables. If outages in your network tend to be longer, you might want to set a shorter carrier delay so that the outages are detected sooner, and the IP route convergence begins and ends sooner.

Examples The following example changes the carrier delay to 5 seconds:

```
Router(config)# interface serial 0
Router(config-if)# carrier-delay 5
```

channel-group (EtherChannel)

To assign and configure a Fast Ethernet interface to an EtherChannel group, use the **channel-group** command in interface configuration mode. To remove the channel-group configuration from the interface, use the **no** form of this command.

Cisco 2600 Series, Cisco 3600 Series, and Cisco 3700 Series Routers

channel-group *port-channel-number* **mode on**

no channel-group

Catalyst Switches

channel-group *port-channel-number* **mode** {**on** | **auto** [**non-silent**] | **desirable** [**non-silent**]}

no channel-group

Syntax Description	
<i>port-channel-number</i>	Specifies the port-channel group number; see the “Usage Guidelines” section for valid values.
mode	Specifies the EtherChannel mode of the interface.
on	Forces the port to channel without Port Aggregation Protocol (PAgP).
auto	Places a port into a passive negotiating state in which the port responds to PAgP packets it receives but does not initiate PAgP packet negotiation.
non-silent	Used with the auto or desirable mode when traffic is expected from the other device.
desirable	Places a port into an active negotiating state in which the port initiates negotiations with other ports by sending PAgP packets.

Defaults No channel groups are assigned.

Command Modes Interface configuration

Command History	Release	Modification
	12.0(7)XE	This command was introduced on Catalyst 6000 family switches.
	12.1(3a)E3	The number of valid values for the <i>port-channel-number</i> argument was changed; see the “Usage Guidelines” section for valid values.
	12.2(2)XT	This command was introduced on the Cisco 2600 series, Cisco 3600 series, and Cisco 3700 series routers.
	12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T on the Cisco 2600 series, the Cisco 3600 series, and the Cisco 3700 series routers.

Usage Guidelines**IP Address for the Physical Interface**

You do not have to disable the IP address that is assigned to a physical interface that is part of a channel group, but Cisco highly recommends doing so.

Layer-2 and Layer-3 Port Channels

You can create both Layer 2 and Layer 3 port channels by entering the **interface port-channel** command or, when the channel-group gets its first physical interface assignment. The port channels are not created at run time, nor are they created dynamically.

You do not have to create a port-channel interface before assigning a physical interface to a channel group. A port-channel interface is automatically created when the channel group gets its first physical interface, if it is not already created.

Propagation of Configuration and Attribute Changes

Any configuration or attribute changes you make to the port-channel interface are propagated to all interfaces within the same channel group as the port channel. (for example, configuration changes are also propagated to the physical interfaces that are not part of the port-channel, but are part of the channel group.)

The on Keyword

When you use the **on** keyword, a usable EtherChannel exists only when a port group in “on” mode is connected to another port group in the “on” mode.

Cisco 2600 Series, Cisco 3600 Series, and Cisco 3700 Series Routers

You do not have to create a port-channel interface before assigning a physical interface to a channel group. A port-channel interface is created automatically when the channel group gets its first physical interface, if it is not already created.

Catalyst Switches

The number of valid values for *port-channel-number* depends on the software release. For software releases prior to Cisco IOS Release 12.1(3a)E3, valid values are from 1 to 256; for Cisco IOS Release 12.1(3a)E3, 12.1(3a)E4, and 12.1(4)E1, valid values are from 1 to 64. Cisco IOS Release 12.1 E and later releases support a maximum of 64 values ranging from 1 to 256.

**Caution**

Do not enable Layer 3 addresses on the physical EtherChannel interfaces. Do not assign bridge groups on the physical EtherChannel interfaces because loops will result.

Examples

This example shows how to add EtherChannel interface 1/0 to the EtherChannel group specified by port-channel 1:

```
Router(config-if)# channel-group 1 mode on
```

Related Commands

Command	Description
interface port-channel	Accesses or creates the IDB port-channel.
show interfaces port-channel	Displays statistics for all interfaces configured.

channel-group (Fast EtherChannel)

To assign a Fast Ethernet interface to a Fast EtherChannel group, use the **channel-group** command in interface configuration mode. To remove a Fast Ethernet interface from a Fast EtherChannel group, use the **no** form of this command.

channel-group *channel-number*

no channel-group *channel-number*

Syntax Description

channel-number Port-channel number previously assigned to the port-channel interface when using the **interface port-channel** global configuration command. The range is 1 to 4.

Defaults

No channel group is configured.

Command Modes

Interface configuration

Command History

Release	Modification
11.1 CA	This command was introduced.

Usage Guidelines

Before you assign a Fast Ethernet interface to a Fast EtherChannel group, you must first create a port-channel interface. To create a port-channel interface, use the **interface port-channel** global configuration command.

If the Fast Ethernet interface has an IP address assigned, you must disable it before adding the Fast Ethernet interface to the Fast EtherChannel. To disable an existing IP address on the Fast Ethernet interface, use the **no ip address** command in interface configuration mode.

The Fast EtherChannel feature allows multiple Fast Ethernet point-to-point links to be bundled into one logical link to provide bidirectional bandwidth of up to 800 Mbps. Fast EtherChannel can be configured between Cisco 7500 series routers and Cisco 7000 series routers with the 7000 Series Route Switch Processor (RSP7000) and 7000 Series Chassis Interface (RSP7000CI) or between a Cisco 7500 series router or a Cisco 7000 series router with the RSP7000 and RSP7000CI and a Catalyst 5000 switch.

A maximum of four Fast Ethernet interfaces can be added to a Fast EtherChannel group.



Caution

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

To display information about the Fast EtherChannel, use the **show interfaces port-channel EXEC** command.

Examples

The following example adds Fast Ethernet 1/0 to the Fast EtherChannel group specified by port-channel 1:

```
Router(config)# interface port-channel 1
Router(config-if)# ip address 1.1.1.10 255.255.255.0
Router(config)# interface fastethernet 1/0/0
```

Related Commands

Command	Description
interface port-channel	Specifies a Fast EtherChannel and enters interface configuration mode.
show interfaces port-channel	Displays the information about the Fast EtherChannel on Cisco 7500 series routers and Cisco 7000 series routers with the RSP7000 and RSP7000CI.

clear aim

To clear the data compression Advanced Interface Module (AIM) daughter card registers and reset the hardware, use the **clear aim** command in privileged EXEC mode.

clear aim *element-number*

Syntax Description

<i>element-number</i>	Number of AIM slot. AIM slots begin with 0.
-----------------------	---

Command Modes

Privileged EXEC

Command History

Release	Modification
12.0(1)T	This command was introduced.

Usage Guidelines

The **clear aim** command is used to reset the data compression AIM hardware. This command is used if the compression Advanced Interface Module (CAIM) hardware becomes “stuck” or hangs for some reason. The CAIM registers are cleared, and the hardware is reset upon execution. All compression history is lost when the CAIM is reset.

This command is supported only on Cisco 2600 series routers.

Examples

The following example shows how to use the **clear aim** command. This command will reset the hardware, flushing the buffers and history for all compression tasks currently under operation:

```
Router# clear aim 0
Router#
1w0d: %CAIM-6-SHUTDOWN: CompressionAim0 shutting down
1w0d: %CAIM-6-STARTUP: CompressionAim0 starting up
```

Related Commands

Command	Description
show pas caim	Displays the IDPROM contents for each AIM board in the Cisco 2600 series routers.
test aim eeprom	Tests the data compression AIM after it is installed in a Cisco 2600 series router.

clear counters

To clear the interface counters, use the **clear counters** command in user EXEC mode.

clear counters [*type number*]

Cisco 7200 Series and 7500 Series with a Packet over SONET Interface Processor

clear counters [*type*] *slot/port*

Cisco 7500 Series with Ports on VIP Cards

clear counters [*type*] *slot/port-adapter/port*

Syntax Description	Argument	Description
	<i>type</i>	(Optional) Specifies the interface type; one of the keywords listed in Table 1 .
	<i>number</i>	(Optional) Specifies the interface counter displayed with the show interfaces command.
	<i>slot</i>	Number of the slot being configured. Refer to the appropriate hardware manual for slot and port information.
	<i>port</i>	Number of the port being configured. Refer to the appropriate hardware manual for slot and port information.
	<i>port-adapter</i>	Number of the port adapter being configured. Refer to the appropriate hardware manual for information about port adapter compatibility.

Command Modes EXEC

Command History	Release	Modification
	10.0	This command was introduced.
	11.2 F	The virtual-access keyword was added.
	11.3	The following keywords were added or modified: <ul style="list-style-type: none"> • vg-anylan • posi keyword changed to pos
	12.2(15)T	The ethernet and serial keywords were removed because the LAN Extension feature is no longer available in Cisco IOS software.

Usage Guidelines This command clears all the current interface counters from the interface unless the optional arguments *type* and *number* are specified to clear only a specific interface type (serial, Ethernet, Token Ring, and so on). [Table 1](#) lists the command keywords and their descriptions.



Note

This command does not clear counters retrieved using Simple Network Management Protocol (SNMP), but only those seen with the **show interface** EXEC command.

Table 1 *clear counters Interface Type Keywords*

Keyword	Interface Type
async	Asynchronous interface
bri	ISDN BRI
dialer	Dialer interface
ethernet	Ethernet interface
fast-ethernet	Fast Ethernet interface
fdi	FDDI
hssi	High-Speed Serial Interface (HSSI)
line	Terminal line
loopback	Loopback interface
null	Null interface
port-channel	Port channel interface
pos	Packet OC-3 interface
serial	Synchronous serial interface
switch	Switch interface
tokenring	Token Ring interface
tunnel	Tunnel interface (IEEE 02.5)
vg-anylan	100VG-AnyLAN port adapter
virtual-access	Virtual-access interface (See <i>Cisco IOS Dial Technologies Command Reference</i> for details on virtual templates.)
virtual-template	Virtual-template interface (See <i>Cisco IOS Dial Technologies Command Reference</i> for details on virtual templates.)
virtual-tokenring	Virtual token ring interface

Examples

The following example clears all interface counters:

```
Router# clear counters
```

The following example clears the Packet OC-3 interface counters on a POSIP card in slot 1 on a Cisco 7500 series router:

```
Router# clear counters pos 1/0
```

The following example clears the interface counters on a Fast EtherChannel interface.

```
Router# clear counter port-channel 1
Clear "show interface" counters on all interfaces [confirm] Y
%CLEAR-5-COUNTERS: Clear counter on all interfaces by console 1
```

Related Commands

Command	Description
show interfaces	Displays the statistical information specific to a serial interface.
show interfaces port-channel	Displays the information about the Fast EtherChannel on Cisco 7500 series routers and Cisco 7000 series routers with the RSP7000 and RSP7000CI.

clear hub

To reset and reinitialize the hub hardware connected to an interface of a Cisco 2505 or Cisco 2507 router, use the **clear hub** command in EXEC mode.

clear hub ethernet *number*

Syntax Description	ethernet	Hub in front of an Ethernet interface.
	<i>number</i>	Hub number to clear, starting with 0. Because there is only one hub, this number is 0.

Command Modes	EXEC
---------------	------

Command History	Release	Modification
	10.3	This command was introduced.

Examples

The following example clears hub 0:

```
Router# clear hub ethernet 0
```

Related Commands	Command	Description
	hub	Enables and configures a port on an Ethernet hub of a Cisco 2505 or Cisco 2507 router.

clear hub counters

To set to zero the hub counters on an interface of a Cisco 2505 or Cisco 2507 router, use the **clear hub counters** command in EXEC mode.

```
clear hub counters [ether number [port [end-port]]]
```

Syntax Description	Parameter	Description
	ether	(Optional) Hub in front of an Ethernet interface.
	<i>number</i>	(Optional) Hub number for which to clear counters. Because there is currently only one hub, this number is 0. If you specify the keyword ether , you must specify the <i>number</i> .
	<i>port</i>	(Optional) 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, this port number indicates the beginning of a port range. If you do not specify a port number, counters for all ports are cleared.
	<i>end-port</i>	(Optional) Ending port number of a range.

Command Modes	Mode
	EXEC

Command History	Release	Modification
	10.3	This command was introduced.

Examples The following example clears the counters displayed in a **show hub** command for all ports on hub 0:

```
Router# clear hub counters ether 0
```

Related Commands	Command	Description
	show hub	Displays information about the hub (repeater) on an Ethernet interface of a Cisco 2505 or Cisco 2507 router.

clear interface

To reset the hardware logic on an interface, use the **clear interface** command in EXEC mode.

```
clear interface type number [name-tag]
```

Cisco 7200 Series and Cisco 7500 Series with a Packet OC-3 Interface Processor

```
clear interface type slot/port
```

Cisco 7500 Series with Ports on VIP Cards

```
clear interface type slot/port-adapter/port
```

Cisco 7500 Series

```
clear interface type slot/port [:channel-group]
```

Cisco 7500 Series with a CT3IP

```
clear interface type slot/port-adapter/port [:t1-channel]
```

Syntax Description

<i>type</i>	Interface type; it is one of the keywords listed in Table 2 .
<i>number</i>	Port, connector, or interface card number.
<i>name-tag</i>	(Optional for use with the RLM feature) Logic name to identify the server configuration so that multiple server configurations can be entered.
<i>slot</i>	Number of the slot being configured. Refer to the appropriate hardware manual for slot and port information.
<i>port</i>	Number of the port being configured. Refer to the appropriate hardware manual for slot and port information.
<i>port-adapter</i>	Number of the port adapter being configured. Refer to the appropriate hardware manual for information about port adapter compatibility.
<i>:channel-group</i>	(Optional) On Cisco 7500 series routers that support channelized T1, specifies the channel number from 0 to 23. This number is preceded by a colon.
<i>:t1-channel</i>	(Optional) For the CT3IP, the T1 channel is a number between 1 and 28. T1 channels on the CT3IP are numbered 1 to 28 rather than the more traditional zero-based scheme (0 to 27) used with other Cisco products. This numbering scheme ensures consistency with telco numbering schemes for T1 channels within channelized T3 equipment.

Command Modes

EXEC

Command History

Release	Modification
10.0	This command was introduced.
11.3	The following keywords were added or modified: <ul style="list-style-type: none"> • vg-anylan keyword added • posi keyword changed to pos
12.0(3)T	The following optional argument was added for the RLM feature: <ul style="list-style-type: none"> • <i>name-tag</i>

Usage Guidelines

Under normal circumstances, you do not need to clear the hardware logic on interfaces.

This command clears all the current interface hardware logic unless the *type* and *number* arguments are specified to clear only a specific interface type (serial, Ethernet, Token Ring, and so on). [Table 2](#) lists the command keywords and their descriptions.

Table 2 *clear interface Type Keywords*

Keyword	Interface Type
async	Async interface
atm	ATM interface
bri	ISDN BRI
ethernet	Ethernet interface
fdi	FDDI
hssi	High-Speed Serial Interface (HSSI)
loopback	Loopback interface
null	Null interface
port-channel	Port channel interface
pos	Packet OC-3 Interface Processor
serial	Synchronous serial interface
switch	Switch interface
tokenring	Token Ring interface
tunnel	Tunnel interface
vg-anylan	100VG-AnyLAN port adapter

Examples

The following example resets the interface logic on HSSI interface 1:

```
Router# clear interface hssi 1
```

The following example resets the interface logic on Packet OC-3 interface 0 on the POSIP in slot 1:

```
Router# clear interface pos 1/0
```

The following example resets the interface logic on T1 0 on the CT3IP in slot 9:

```
Router# clear interface serial 9/0/0:0
```

The following example resets the interface logic on Fast Etherchannel interface 1:

```
Router# clear interface port-channel 1
```

The following example demonstrates the use of the **clear interface** command with the RLM feature:

```
Router# clear interface loopback 1
```

```
Router#
02:48:52: rlm 1: [State_Up, rx ACTIVE_LINK_BROKEN] over link [10.1.1.1(Loopback1),
10.1.4.1]
02:48:52: rlm 1: link [10.1.1.2(Loopback2), 10.1.4.2] requests activation
02:48:52: rlm 1: link [10.1.1.1(Loopback1), 10.1.4.1] is deactivated
02:48:52: rlm 1: link [10.1.1.1(Loopback1), 10.1.4.1] = socket[10.1.1.1, 10.1.4.1]
02:48:52: rlm 1: [State_Recover, rx USER_SOCKET_OPENED] over link [10.1.1.1(Loopback1),
10.1.4.1] for user RLM_MGR
02:48:52: rlm 1: link [10.1.1.1(Loopback1), 10.1.4.1] is opened
02:48:52: rlm 1: link [10.1.1.1(Loopback1), 10.1.5.1] = socket[10.1.1.1, 10.1.5.1]
02:48:52: rlm 1: [State_Recover, rx USER_SOCKET_OPENED] over link [10.1.1.1(Loopback1),
10.1.5.1] for user RLM_MGR
02:48:52: rlm 1: link [10.1.1.1(Loopback1), 10.1.5.1] is opened
02:48:52: rlm 1: [State_Recover, rx START_ACK] over link [10.1.1.2(Loopback2), 10.1.4.2]
02:48:52: rlm 1: link [10.1.1.2(Loopback2), 10.1.4.2] is activated
02:48:52: rlm 1: [State_Up, rx LINK_OPENED] over link [10.1.1.1(Loopback1), 10.1.4.1]
```

```
Router# show rlm group 1 status
```

```
RLM Group 1 Status
User/Port: RLM_MGR/3000
Link State: Up          Last Link Status Reported: Up_Recovered
Next tx TID: 4         Last rx TID: 0
Server Link Group[r1-server]:
  link [10.1.1.1(Loopback1), 10.1.4.1] = socket[standby, 10.1.1.1, 10.1.4.1]
  link [10.1.1.2(Loopback2), 10.1.4.2] = socket[active, 10.1.1.2, 10.1.4.2]
Server Link Group[r2-server]:
  link [10.1.1.1(Loopback1), 10.1.5.1] = socket[opening, 10.1.1.1, 10.1.5.1]
  link [10.1.1.2(Loopback2), 10.1.5.2] = socket[opening, 10.1.1.2, 10.1.5.2]
```

```
Router#
Router#
02:49:52: rlm 1: [State_Up, rx UP_RECOVERED_MIN_TIMEOUT]
02:49:52: rlm 1: link [10.1.1.1(Loopback1), 10.1.4.1] requests activation
02:49:52: rlm 1: [State_Switch, rx SWITCH_ACK] over link [10.1.1.1(Loopback1), 10.1.4.1]
02:49:52: rlm 1: link [10.1.1.2(Loopback2), 10.1.4.2] is deactivated
02:49:52: rlm 1: link [10.1.1.1(Loopback1), 10.1.4.1] is activated
```

Related Commands

Command	Description
interface	Defines the IP addresses of the server, configures an interface type, and enters interface configuration mode.
show rlm group	Displays the status of the RLM group.
shutdown (RLM)	Shuts down all of the links under the RLM group.

clear interface fastethernet

To reset the controller for a specified Fast Ethernet interface, use the **clear interface fastethernet** command in privileged EXEC mode.

Cisco 4500 and Cisco 4700 series

```
clear interface fastethernet number
```

Cisco 7200 and Cisco 7500 series

```
clear interface fastethernet slot/port
```

Cisco 7500 series

```
clear interface fastethernet slot/port-adapter/port
```

Syntax Description		
<i>number</i>		Port, connector, or interface card number. On a Cisco 4500 or Cisco 4700 router, specifies the number of the network processor module (NPM) number. The numbers are assigned at the factory at the time of installation or when added to a system.
<i>slot</i>		Number of the slot being configured. Refer to the appropriate hardware manual for slot and port information.
<i>port</i>		Number of the port being configured. Refer to the appropriate hardware manual for slot and port information.
<i>port-adapter</i>		Number of the port adapter being configured. Refer to the appropriate hardware manual for information about port adapter compatibility.

Command Modes	
	Privileged EXEC

Command History	Release	Modification
	11.2	This command was introduced.

Examples

Cisco 4500

The following example resets the controller for Fast Ethernet interface 0 on a Cisco 4500:

```
Router# clear interface fastethernet 0
```

Cisco 7200 and Cisco 7500

The following example resets the controller for the Fast Ethernet interface located in slot 1 port 0 on a Cisco 7200 series router or Cisco 7500 series router:

```
Router# clear interface fastethernet 1/0
```

Cisco 7500

The following example resets the controller for the Fast Ethernet interface located in slot 1 port adapter 0 port 0 on a Cisco 7500 series routers:

```
Router# clear interface fastethernet 1/0/0
```

Related Commands

Command	Description
clear counters	Clears the interface counters.
show interfaces	Displays statistics for all interfaces configured on the router or access server.
show interfaces serial	Displays information about a serial interface.

clear interface serial

To reset the statistical information specific to a serial interface, use the **clear interface serial** command in user EXEC mode.

clear interface serial *dial-shelf/slot/t3-port:t1-num:chan-group*

Syntax Description

<i>dial-shelf</i>	Dial shelf chassis in the Cisco AS5800 access server containing the CT3 interface card.
<i>slot</i>	Location of the CT3 interface card in the dial shelf chassis.
<i>t3-port</i>	T3 port number. The only valid value is 0.
<i>:t1-num</i>	T1 timeslot in the T3 line. The value can be from 1 to 28.
<i>:chan-group</i>	Channel group identifier.

Command Modes

EXEC

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines

The **clear interface serial** command clears the interface hardware. To reset the counters for an interface, use the **clear counters** command with the **serial** keyword specified. To confirm at the prompt, use the **show interfaces serial** command.

Examples

The following example clears the interface hardware, disconnecting any active lines:

```
Router# clear interface serial 1/4/0:2:23
Router#
```

Related Commands

Command	Description
clear counters	Clears the interface counters.
show interfaces	Displays statistics for all interfaces configured on the router or access server.
show interfaces fastethernet	Displays information about a fastethernet interface.

clear ipc statistics

To clear all interprocess communication (IPC) statistics, use the **clear ipc statistics** command in privileged EXEC mode.

clear ipc statistics

Syntax Description This command has no arguments or keywords.

Command Modes Privileged EXEC

Command History	Release	Modification
	12.2(15)T	This command was introduced.

Usage Guidelines The **clear ipc statistics** command clears all the IPC statistics and is useful for troubleshooting issues with IPC services.

Examples The following example shows how to clear all of the statistics used by IPC services. A **show ipc status** command is issued first to display the current IPC counters for a local IPC server. The **clear ipc statistics** command is then entered to clear and reset the counters. A final **show ipc status** command is issued to show that all the counters, except those counters that show the packets sent since the clearing, are reset to zero.

```
Router# show ipc status

IPC System Status

Time last IPC stat cleared : never

This processor is the IPC master server.
Do not drop output of IPC frames for test purposes.

1000 IPC Message Headers Cached.
```

	Rx Side	Tx Side
Total Frames	189	140
Total from Local Ports	189	70
Total Protocol Control Frames	70	44
Total Frames Dropped	0	0

```

Service Usage

Total via Unreliable Connection-Less Service      145      0
Total via Unreliable Sequenced Connection-Less Svc  0        0
Total via Reliable Connection-Oriented Service    44       70
```

```

IPC Protocol Version 0

Total Acknowledgements          70          44
Total Negative Acknowledgements  0           0

Device Drivers

Total via Local Driver           0           0
Total via Platform Driver        0          70
Total Frames Dropped by Platform Drivers  0           0

Reliable Tx Statistics

Re-Transmission                  0
Re-Tx Timeout                    0

Rx Errors                          Tx Errors

Unsupp IPC Proto Version         0 Tx Session Error          0
Corrupt Frame                    0 Tx Seat Error              0
Duplicate Frame                  0 Destination Unreachable  0
Out-of-Sequence Frame           0 Tx Test Drop              0
Dest Port does Not Exist        0 Tx Driver Failed          0
Rx IPC Msg Alloc Failed          0 Ctrl Frm Alloc Failed    0
Unable to Deliver Msg           0

Buffer Errors                      Misc Errors

IPC Msg Alloc                    0 IPC Open Port              0
Emer IPC Msg Alloc               0 No HWQ                     0
IPC Frame PakType Alloc          0 Hardware Error            0
IPC Frame MemD Alloc             0

Tx Driver Errors

No Transport                      0
MTU Failure                       0
Dest does not Exist              0

Router# clear ipc statistics

Router# show ipc status

IPC System Status

Time last IPC stat cleared : 00:00:03

This processor is the IPC master server.
Do not drop output of IPC frames for test purposes.

1000 IPC Message Headers Cached.

Rx Side      Tx Side
Total Frames 26          0
Total from Local Ports 26          0
Total Protocol Control Frames 0          0
Total Frames Dropped 0          0

```

```

Service Usage

Total via Unreliable Connection-Less Service          26          0
Total via Unreliable Sequenced Connection-Less Svc    0           0
Total via Reliable Connection-Oriented Service        0           0

IPC Protocol Version 0

Total Acknowledgements                               0           0
Total Negative Acknowledgements                       0           0

                        Device Drivers

Total via Local Driver                                0           0
Total via Platform Driver                             0           0
Total Frames Dropped by Platform Drivers              0           0

                        Reliable Tx Statistics

Re-Transmission                                       0
Re-Tx Timeout                                         0

                        Rx Errors                                Tx Errors

Unsupp IPC Proto Version                             0 Tx Session Error                                0
Corrupt Frame                                         0 Tx Seat Error                                    0
Duplicate Frame                                        0 Destination Unreachable                        0
Out-of-Sequence Frame                                0 Tx Test Drop                                    0
Dest Port does Not Exist                             0 Tx Driver Failed                                0
Rx IPC Msg Alloc Failed                              0 Ctrl Frm Alloc Failed                          0
Unable to Deliver Msg                                0

                        Buffer Errors                            Misc Errors

IPC Msg Alloc                                         0 IPC Open Port                                    0
Emer IPC Msg Alloc                                    0 No HWQ                                            0
IPC Frame PakType Alloc                              0 Hardware Error                                  0
IPC Frame MemD Alloc                                  0

                        Tx Driver Errors

No Transport                                          0
MTU Failure                                           0
Dest does not Exist                                  0

```

Related Commands

Command	Description
show ipc	Displays IPC statistics.

cmt connect

To start the processes that perform the connection management (CMT) function and allow the ring on one fiber to be started, use the **cmt connect** command in EXEC mode.

cmt connect [**fdi** [*port* | *slot/port*] [**phy-a** | **phy-b**]]

Syntax Description

fdi	(Optional) Identifies this as a FDDI interface.
<i>port</i>	(Optional) Number of the port being configured. Refer to the appropriate hardware manual for slot and port information.
<i>slot</i>	(Optional) Number of the slot being configured. Refer to the appropriate hardware manual for slot and port information.
phy-a	(Optional) Selects Physical Sublayer A.
phy-b	(Optional) Selects Physical Sublayer B.

Command Modes

EXEC

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines

In normal operation, the FDDI interface is operational once the interface is connected and configured. The **cmt connect** command allows the operator to start the processes that perform the CMT function.

The **cmt connect** command is not needed in the normal operation of FDDI; this command is used mainly in interoperability tests.

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

Examples

The following examples demonstrate use of the **cmt connect** command for starting the CMT processes on the FDDI ring.

The following command starts all FDDI interfaces:

```
Router# cmt connect
```

The following command starts both fibers on FDDI interface unit 0:

```
Router# cmt connect fddi 0
```

The following command on the Cisco 7200 series or Cisco 7500 series starts both fibers on FDDI interface unit 0:

```
Router# cmt connect fddi 1/0
```

The following command starts only Physical Sublayer A on FDDI interface unit 0:

```
Router# cmt connect fddi 0 phy-a
```

The following command on Cisco 7500 series routers starts only Physical Sublayer A on FDDI interface unit 0:

```
Router# cmt connect fddi 1/0 phy-a
```

cmt disconnect

To stop the processes that perform the connection management (CMT) function and allow the ring on one fiber to be stopped, use the **cmt disconnect** command in EXEC mode.

cmt disconnect [**fddi** [*port* | *slot/port*] [**phy-a** | **phy-b**]]

Syntax Description		
fddi	(Optional)	Identifies this as a FDDI interface.
<i>port</i>	(Optional)	Number of the port being configured. Refer to the appropriate hardware manual for slot and port information.
<i>slot</i>	(Optional)	Number of the slot being configured. Refer to the appropriate hardware manual for slot and port information.
phy-a	(Optional)	Selects Physical Sublayer A.
phy-b	(Optional)	Selects Physical Sublayer B.

Command Modes EXEC

Command History	Release	Modification
	10.0	This command was introduced.

Usage Guidelines

In normal operation, the FDDI interface is operational once the interface is connected and configured, and is turned off using the **shutdown** command in interface configuration mode. The **cmt disconnect** command allows the operator to stop the processes that perform the CMT function and allow the ring on one fiber to be stopped.

The **cmt disconnect** command is not needed in the normal operation of FDDI; this command is used mainly in interoperability tests.

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

Examples

The following examples demonstrate use of the **cmt disconnect** command for stopping the CMT processes on the FDDI ring.

The following command stops all FDDI interfaces:

```
Router# cmt disconnect
```

The following command stops both fibers on FDDI interface unit 0:

```
Router# cmt disconnect fddi 0
```

The following command on the Cisco 7200 series or Cisco 7500 series stops both fibers on FDDI interface unit 0:

```
Router# cmt disconnect fddi 1/0
```

The following command stops only Physical Sublayer A on the FDDI interface unit 0. This command causes the FDDI media to go into a wrapped state so that the ring will be broken.

```
Router# cmt disconnect fddi 0 phy-a
```

The following command on the Cisco 7500 series stops only Physical Sublayer A on FDDI interface unit 0 in slot 1. This command causes the FDDI media to go into a wrapped state so that the ring will be broken.

```
Router# cmt disconnect fddi 1/0 phy-a
```

compress

To configure software compression for Link Access Procedure, Balanced (LAPB), PPP, and High-Level Data Link Control (HDLC) encapsulations, use the **compress** command in interface configuration mode. On Cisco 7200 series routers and Cisco 7500 series routers, hardware compression on the compression service adapter (CSA) is supported for PPP links. To disable compression, use the **no** form of this command.

```
compress {predictor | stac}
```

```
no compress {predictor | stac}
```

Cisco VIP2 Cards

```
compress {predictor | stac [distributed | software]}
```

```
[no] compress {predictor | stac [distributed | software]}
```

Cisco 7200 Series and Cisco 7500 Series

```
compress {predictor | stac [csa slot | software]}
```

```
[no] compress {predictor | stac [csa slot | software]}
```

PPP Encapsulation

```
compress [predictor | stac | mppc [ignore-pfc]]
```

```
[no] compress [predictor | stac | mppc [ignore-pfc]]
```

Syntax Description

predictor	Specifies that a predictor (RAND) compression algorithm will be used on LAPB and PPP encapsulation. Compression is implemented in the software installed in the router's main processor.
stac	<p>Specifies that a Stacker (LZS) compression algorithm will be used on LAPB, HDLC, and PPP encapsulation. For all platforms except Cisco 7200 series and platforms that support the Virtual Interface Processor 2 (VIP2), compression is implemented in the software installed in the router's main processor.</p> <p>On Cisco 7200 series and on VIP2s in Cisco 7500 series, specifying the compress stac command with no options causes the router to use the fastest available compression method for PPP encapsulation only:</p> <ul style="list-style-type: none"> • If the router contains a compression service adapter (CSA), compression is performed in the CSA hardware (hardware compression). • If a CSA is not available, compression is performed in the software installed on the VIP2 (distributed compression). • If a VIP2 is not available, compression is performed in the router's main processor (software compression).
distributed	(Optional) Specifies that compression is implemented in the software that is installed in a VIP2. If the VIP2 is not available, compression is performed in the router's main processor (software compression).

software	(Optional) Specifies that compression is implemented in the Cisco IOS software installed in the router's main processor.
csa slot	(Optional) Specifies the CSA to use for a particular interface.
mppc	(Optional) Specifies that the MPPC compression algorithm be used.
ignore-pfc	(Optional) Specifies that the protocol field compression flag negotiated through LCP will be ignored.

Defaults

Compression is disabled.

Command Modes

Interface configuration

Command History

Release	Modification
10.3	This command was introduced.
11.3 P	The following keywords were added: <ul style="list-style-type: none"> • distributed • software • csa slot
11.3 T	The following keywords were added: <ul style="list-style-type: none"> • mppc • ignore-pfc

**Note**

This command replaces the **compress predictor** command.

Usage Guidelines**Point-to-Point Compression**

Compression reduces the size of frames through lossless data compression. You can configure point-to-point software compression for all LAPB, PPP, and HDLC encapsulations. The compression algorithm used is a predictor algorithm (the RAND compression algorithm), which uses a compression dictionary to predict what the next character in the frame will be.

End-point devices must be configured to use the same compression method (predictor, Stacker or MPPC).

HDLC encapsulations supports the Stacker compression algorithm. PPP and LAPB encapsulations support both predictor and Stacker compression algorithms.

MPPC Compression

The **compress** command using the **mppc** and **ignore-pfc** options support compression between Cisco routers and access servers and Microsoft clients, such as Windows 95 and Windows NT. MPPC implements an LZ-based compression algorithm that uses a compression dictionary to compress PPP packets. The **ignore-pfc** keyword instructs the router to ignore the protocol field compression flag negotiated by LCP. For example, the standard protocol field value for IP is 0x0021 when compression is disabled and 0x21 when compression is enabled. When the **ignore-pfc** option is enabled, the router will continue to use the uncompressed value (0x0021). Using the **ignore-pfc** option is helpful for some

asynchronous driver devices that use an uncompressed protocol field (0x0021), even though the pfc is negotiated between peers. If protocol rejects are displayed when the **debug ppp negotiation** command is enabled, setting the **ignore-pfc** option may remedy the problem.

HDLC Encapsulations

For HDLC encapsulations, you can specify a Stacker compression algorithm by using the **stac** keyword. PPP and LAPB encapsulations support both predictor and Stacker compression algorithms.

Public Data Network Connections

Compression requires that both ends of the serial link be configured to use compression. You should never enable compression for connections to a public data network.

Cisco 7200 and 7500 Series

Using CSA hardware compression on Cisco 7200 series routers and Cisco 7500 series routers removes the compression and decompression responsibilities from the VIP2 or the main processor installed in the router. By using the **compress stac** command, the router determines the fastest compression method available on the router.

When using hardware compression on Cisco 7200 series routers with multiple CSAs, you can optionally specify which CSA is used by the interface to perform compression. If no CSA is specified, the router determines which CSA is used. On Cisco 7500 series routers, the router uses the CSA on the same VIP2 as the interface.

System Performance



Caution

When compression is performed in software installed in the router's main processor, it might affect system performance significantly. We recommend that you disable compression if the CPU load exceeds 40 percent. To display the CPU load, use the **show process cpu EXEC** command.

If the majority of your traffic is already compressed files, we recommend that you not use compression. If the files are already compressed, the additional processing time spent in attempting unsuccessfully to compress them again will slow system performance.

[Table 3](#) provides general guidelines for deciding which compression type to select.

Table 3 *Compression Guidelines*

Situation	Compression Type to Use
Bottleneck is caused by the load on the router.	Predictor
Bottleneck is the result of line bandwidth or hardware compression on the CSA is available.	Stacker
Most files are already compressed.	None

Software compression makes heavy demands on the router's processor. The maximum compressed serial line rate depends on the type of Cisco router that you are using and which compression algorithm you specify. [Table 4](#) shows a summary of the compressed serial line rates for software compression. The maximums shown in [Table 4](#) apply to the "combined" serial compressed load on the router. For example, a Cisco 4000 series router could handle four 64-kbps lines using Stacker compression or one 256-kbps line. These maximums also assume that there is very little processor load on the router aside from compression. Lower these numbers when the router is required to do other processor-intensive tasks.

Table 4 Combined Compressed Serial Line Rates (Software Compression)

Compression Method	Cisco 1000 Series	Cisco 3000 Series	Cisco 4000 Series	Cisco 4500 Series	Cisco 4700 Series	Cisco 7000 Family
Stacker (kbps)	128	128	256	500	T1	256
Predictor (kbps)	256	256	500	T1	2xT1	500

Hardware compression can support a combined line rate of 16 Mbps.

Cisco recommends that you do not adjust the maximum transmission unit (MTU) for the serial interface and the LAPB maximum bits per frame (N1) parameter.

**Note**

The best performance data compression algorithms adjust their compression methodology as they identify patterns in the data. To prevent data loss and support this adjustment process, the compression algorithm is run over LAPB to ensure that everything is sent in order, with no missing data and no duplicate data.

**Note**

For information on configuring Frame Relay compression, refer to the “Configuring Frame Relay” chapter in the *Cisco IOS Wide-Area Networking Configuration Guide*.

Examples

The following example enables hardware compression and PPP encapsulation on serial interface 3/1/0.

```
Router(config)# interface serial 3/1/0
Router(config-if)# encapsulate ppp
Router(config-if)# compress stac
```

The following example enables predictor compression on serial interface 0 for a LAPB link:

```
Router(config)# interface serial 0
Router(config-if)# encapsulation lapb
Router(config-if)# compress predictor
Router(config-if)# mtu 1509
Router(config-if)# lapb n1 12072
```

The following example enables Stacker compression on serial interface 0 for a LAPB link. This example does not set the MTU size and the maximum bits per frame (N1); we recommend that you do not change those LAPB parameters for Stacker compression:

```
Router(config)# interface serial 0
Router(config-if)# encapsulation lapb
Router(config-if)# compress predictor
```

The following example configures BRI interface 0 to perform MPPC:

```
Router(config)# interface BRI0
Router(config-if)# ip unnumbered ethernet0
Router(config-if)# encapsulation ppp
Router(config-if)# isdn spid1 5551234
Router(config-if)# dialer map ip 172.21.71.74 5551234
Router(config-if)# dialer-group 1
Router(config-if)# compress mppc
```

The following example configures asynchronous interface 1 to implement MPPC and ignore the protocol field compression flag negotiated by LCP:

```
Router(config)# interface async1
Router(config-if)# ip unnumbered ethernet0
Router(config-if)# encapsulation ppp
Router(config-if)# async default routing
Router(config-if)# async dynamic routing
Router(config-if)# async mode interactive
Router(config-if)# peer default ip address 172.21.71.74
Router(config-if)# compress mppc ignore-pfc
```

Related Commands

Command	Description
encapsulation	Sets the encapsulation method used by the interface.
encapsulation x25	Specifies operation of a serial interface as an X.25 device.
exec	Allows an EXEC process on a line.
show compress	Displays compression statistics.
show processes	Displays information about the active processes.

compress mppc

To configure compression using the Microsoft PPC (MPPC) compression algorithm on your data compression Advanced Interface Module (AIM) for the Cisco 2600 series router, use the **compress mppc** command in interface configuration mode. The MPPC compression algorithm is used to exchange compressed information with a Microsoft NT remote access server. To disable compression, use the **no** form of this command.

compress mppc

no compress

Syntax Description This command has no keywords or arguments.

Defaults Disabled

Command Modes Interface configuration

Command History	Release	Modification
	12.0(1)T	This command was introduced.

Usage Guidelines When configuring PPP on a serial interface, you can use hardware compression on the data compression AIM daughter card for MPPC if one is installed; otherwise you can use software compression.

Examples The following example shows how to configure the data compression AIM daughtercard for MPPC:

```
Router(config-if)# encapsulate ppp
Router(config-if)# compress mppc
```

Related Commands	Command	Description
	clear aim	Clears data compression AIM registers and resets the hardware.
	compress stac caim	Specifies the exact hardware compression resource preferred.
	encapsulation	Sets the encapsulation method used by the interface.
	show compress	Displays compression statistics.
	show pas caim	Displays debug information about the data compression AIM daughtercard.
	show processes	Displays information about the active processes.

compress stac caim

To specify the hardware compression, use the **compress stac caim** command in interface configuration mode. To disable compression, use the **no** form of this command.

compress stac caim *element-number*

no compress stac caim *element-number*

Syntax Description	<i>element-number</i>	Interface on which compression is enabled. AIM interfaces begin with 0.
Defaults	Disabled	
Command Modes	Interface configuration	
Command History	Release	Modification
	12.0(1)T	This command was introduced.

Usage Guidelines

Hardware Compression

If the router contains a data compression Advanced Interface Module (CAIM), compression is performed in the CAIM hardware.

Using hardware compression in the AIM frees the main processor of the router for other tasks. You can also configure the router to use the Compression Port Module to perform compression by using the distributed option or to use the router's main processor by using the software option. If the Compression Port Module compression is performed in the main processor of the router.

Software Compression

If the CAIM is not available, compression is performed in the main processor of the router.

When compression is performed by the software installed in the router's main memory, system performance might be affected significantly. It is recommended that you disable compression in the main processor if the router CPU load exceeds 40 percent. To display the CPU load, use the **show process cpu** command in EXEC mode.

Examples

The following example specifies that hardware compression should be activated for CAIM element 0:

```
Router(config-if)# encapsulation ppp
Router(config-if)# compress stac caim 0
Router(config)# Ctrl-Z
```

Related Commands

Command	Description
clear aim	Clears data compression AIM registers and resets the hardware.
encapsulation	Sets the encapsulation method used by the interface.
show compress	Displays compression statistics.
show pas caim	Displays debug information about the data compression AIM daughtercard.

crc

To set the length of the cyclic redundancy check (CRC) on a Fast Serial Interface Processor (FSIP) or HSSI Interface Processor (HIP) of the Cisco 7500 series routers or on a 4-port serial adapter of the Cisco 7200 series routers, use the **crc** command in interface configuration mode. To set the CRC length to 16 bits, use the **no** form of this command.

crc *size*

no crc

Syntax Description	<i>size</i>	CRC size (16 or 32 bits). The default is 16 bits.
Defaults	16 bits	
Command Modes	Interface configuration	
Command History	Release	Modification
	10.0	This command was introduced.
Usage Guidelines	<p>All interfaces use a 16-bit CRC by default, but also support a 32-bit CRC. CRC is an error-checking technique that uses a calculated numeric value to detect errors in transmitted data. The designators 16 and 32 indicate the length (in bits) of the frame check sequence (FCS). A CRC of 32 bits provides more powerful error detection, but adds overhead. Both the sender and receiver must use the same setting.</p> <p>CRC-16, the most widely used throughout the United States and Europe, is used extensively with WANs. CRC-32 is specified by IEEE 802 and as an option by some point-to-point transmission standards. It is often used on Switched Multimegabit Data Service (SMDS) networks and LANs.</p>	
Examples	<p>The following example enables the 32-bit CRC on serial interface 3/0:</p> <pre>Router(config)# interface serial 3/0 Router(config-if)# crc 32</pre>	

crc4

To enable generation of CRC4 (per ITU Recommendation G.704 and G.703) to improve data integrity, use the **crc4** command in interface configuration mode. To disable this feature, use the **no** form of this command.

crc4

no crc4

Syntax Description This command has no arguments or keywords.

Defaults Disabled

Command Modes Interface configuration

Command History	Release	Modification
	10.3	This command was introduced.
	11.1 CA	This command was modified to include the Cisco 7200 series router and the E1-G.703/G.704 serial port adapter

Usage Guidelines This command applies to a Cisco 4000 router and to Cisco 7200 series, Cisco 7000 series, and Cisco 7500 series routers. This command is supported on the Fast Serial Interface Processor (FSIP) and the E1-G.703/G.704 serial port adapter.

This command is useful for checking data integrity while operating in framed mode. CRC4 provides additional protection for a frame alignment signal under noisy conditions. For data transmission at E1 (2.048 Mbps), the G.704 standard suggests 4 bits CRC. Refer to CCITT Recommendation G.704 for a definition of CRC4.

You can also use the **crc** command to set the CRC size for the High-Level Data Link Control (HDLC) controllers.

Examples The following example enables CRC4 generation on the E1-G.703/G.704 serial port adapter and also sets the CRC size to 32 bits:

```
Router(config)# interface serial 0/0
Router(config-if)# crc 32
Router(config-if)# crc4
```

crc bits 5

To enable generation of CRC5 (per ITU Recommendation G.704 and G.703) to improve data integrity, use the **crc bits 5** command in interface configuration mode. To disable this feature, use the **no** form of this command.

crc bits 5

no crc bits 5

Syntax Description This command has no arguments or keywords.

Defaults The default is no CRC5 checking.

Command Modes Interface configuration

Command History	Release	Modification
	11.1 CA	This command was introduced.

Usage Guidelines This command is available for the JT2 6.3-MHz serial port adapter (PA-2JT2) on the second-generation Versatile Interface Processor (VIP2), in Cisco 7500 series routers, and in Cisco 7000 series routers with the Cisco 7000 series Route Switch Processor (RSP7000) and the Cisco 7000 series Chassis Interface (RSP7000CI).

This command is useful for checking data integrity while operating in framed mode. CRC5 provides additional protection for a frame alignment signal under noisy conditions. For data transmission at JT2 (6.312 Mbps), the G.704 standard suggests 5 bits CRC. Refer to ITU Recommendation G.704 for a definition of CRC5.

You can also use the **crc** command to set the CRC size for the High-Level Data Link Control (HDLC) controllers.

Examples The following example enables CRC 5 generation on the PA-2JT2 port adapter and also sets the CRC size to 32 bits:

```
Router(config)# interface serial 0/0
Router(config-if)# crc 32
Router(config-if)# crc bits 5
```

Related Commands

Command	Description
clns routing	Enables routing of CLNS packets.
debug ctunnel	Displays debug messages for the IP over a CLNS Tunnel feature.
interface ctunnel	Creates a virtual interface to transport IP over a CLNS tunnel.
ip address	Sets a primary or secondary IP address for an interface.
ip routing	Enables IP routing.
show interfaces ctunnel	Displays information about an IP over CTunnel

cut-through

To configure the interfaces on the PA-12E/2FE port adapter to use cut-through switching technology between interfaces within the same bridge group, use the **cut-through** command in interface configuration mode. To return each interface to store-and-forward switching, use the **no** form of this command.

cut-through [receive | transmit]

no cut-through

Syntax Description	receive	(Optional) Selects cut-through switching technology on received data.
	transmit	(Optional) Selects cut-through switching technology on transmitted data.

Defaults Store-and-forward switching technology (that is, no cut-through)

Command Modes Interface configuration

Command History	Release	Modification
	11.2 P	This command was introduced.

Usage Guidelines Cut-through mode allows switched packets to be transmitted after 64 bytes are received. The transmission of the packets can start before the end of the packet arrives. This reduces the time spent in the switch, but allows packets to be transmitted with bad cyclical redundancy check (CRCs), because the transmission is initiated before the CRC is received or checked. Store-and-forward mode waits for the entire packet to be received before that packet is forwarded, but will check the CRC before starting transmission.

The PA-12E/2FE port adapter offloads Layer 2 switching from the host CPU by using store-and-forward or cut-through switching technology between interfaces within the same virtual LAN (VLAN) on the PA-12E/2FE port adapter. The PA-12E/2FE port adapter supports up to four VLANs (bridge groups).

Examples The following example configures interface 3/0 for cut-through switching:

```
Router(config)# interface fastethernet 3/0
Router(config-if)# bridge-group 10
Router(config-if)# cut-through
Router(config-if)# no shutdown
Router(config-if)# exit
Router(config)#
```

Related Commands	Command	Description
	more	Displays a specified file.