

access-list (standard)

Use the **access-list** global configuration command to establish MAC address access lists. Use the **no** form of this command to remove a single access list entry.

access-list *access-list-number* { **permit** | **deny** } *address mask*

no access-list *access-list-number*

Syntax Description		
<i>access-list-number</i>		Integer from 700 to 799 that you select for the list.
permit		Permits the frame.
deny		Denies the frame.
<i>address mask</i>		48-bit MAC addresses written in dotted triplet form. The ones bits in the <i>mask</i> argument are the bits to be ignored in the <i>address</i> value.

Defaults No MAC address access lists are established.

Command Modes Global configuration

Command History	Release	Modification
	10.0	This command was introduced.

Related Commands	Command	Description
	access-list (type-code-ibm)	Builds type-code access lists.

access-list (type-code)

Use the **access-list** global configuration command to build type-code access lists. Use the **no** form of this command to remove a single access list entry.

access-list *access-list-number* {**permit** | **deny**} *type-code wild-mask*

no access-list *access-list-number*

Syntax Description		
	<i>access-list-number</i>	User-selectable number between 200 and 299 that identifies the list.
	permit	Permits the frame.
	deny	Denies the frame.
	<i>type-code</i>	16-bit hexadecimal number written with a leading "0x"; for example, 0x6000. You can specify either an Ethernet type code for Ethernet-encapsulated packets, or a DSAP/SSAP pair for 802.3 or 802.5-encapsulated packets.
	<i>wild-mask</i>	16-bit hexadecimal number whose ones bits correspond to bits in the <i>type-code</i> argument that should be ignored when making a comparison. (A mask for a DSAP/SSAP pair should always be at least 0x0101. This is because these two bits are used for purposes other than identifying the SAP codes.)

Defaults No type-code access lists are built.

Command Modes Global configuration

Command History	Release	Modification
	10.0	This command was introduced.

Usage Guidelines Type-code access lists can have an impact on system performance; therefore, keep the lists as short as possible and use wildcard bit masks whenever possible.

Access lists are evaluated according to the following algorithm:

- If the packet is Ethernet Type II or SNAP, the type-code field is used.
- Other packet type, then the LSAP is used.

If the length/type field is greater than 1500, the packet is treated as an LSAP packet unless the DSAP and SSAP fields are AAAA. If the latter is true, the packet is treated using type-code filtering.

If you have both Ethernet Type II and LSAP packets on your network, you should set up access lists for both.

Use the last item of an access list to specify a default action; for example, permit everything else or deny everything else. If nothing else in the access list matches, the default action is normally to deny access; that is, filter out all other type codes.

Related Commands	Command	Description
	access-list (XNS extended)	Defines an extended XNS access list.
	access-list (XNS standard)	Defines a standard XNS access list.

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** interface configuration command. Use the **no** form of this command, to disable authentication.

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. Up to eight alphanumeric characters are accepted.						
Defaults	Authentication is disabled.						
Command Modes	Interface configuration						
Command History	<table border="1"> <thead> <tr> <th>Release</th> <th>Modification</th> </tr> </thead> <tbody> <tr> <td>11.1 CC</td> <td>This command was introduced.</td> </tr> </tbody> </table>	Release	Modification	11.1 CC	This command was introduced.		
Release	Modification						
11.1 CC	This command was introduced.						
Usage Guidelines	<p>Use the aps authenticate command to ensure that only valid packets are accepted on the OOB communication channel.</p> <p>The aps authenticate command must be configured on both the working and protect interfaces.</p>						
Examples	<p>The following example enables authentication on POS interface 0 in slot 4:</p> <pre>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#</pre>						
Related Commands	<table border="1"> <thead> <tr> <th>Command</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td>aps protect</td> <td>Enables a POS interface as a protect interface.</td> </tr> <tr> <td>aps working</td> <td>Configures a POS interface as a working interface.</td> </tr> </tbody> </table>	Command	Description	aps protect	Enables a POS interface as a protect interface.	aps working	Configures a POS interface as a working interface.
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** interface configuration command. Use the **no** form of this command, to cancel the switch.

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 1
router(config-if)# aps force 1
router(config-if)# exit
router(config)# exit
router#
```

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** interface configuration command. Use the **no** form of this command to remove a group.

aps group *group-number*

no aps group *group-number*

Syntax Description

<i>group-number</i>	Number of the group. The default <i>group-number</i> is 0.
---------------------	--

Defaults

No groups exist.



Note

0 is a valid group number; **aps group 0** 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 7.7.7.6 255.255.255.0
router(config)# interface pos 3/0/0
router(config-if)# aps group 10
router(config-if)# aps working 1
router(config)# interface pos 2/0/1
router(config-if)# aps group 20
router(config-if)# aps protect 1 7.7.7.7
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)# interface pos 4/0/0
router(config-if)# aps group 10
router(config-if)# aps protect 1 7.7.7.6
router(config)# interface pos 5/0/0
router(config-if)# aps group 20
router(config-if)# aps working 1
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 lockdown

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

aps lockdown *circuit-number*

no aps lockdown *circuit-number*

Syntax Description	<i>circuit-number</i>	Number of the circuit to lockdown.						
Defaults	No lockdown exists.							
Command Modes	Interface configuration							
Command History	<table border="1"> <thead> <tr> <th>Release</th> <th>Modification</th> </tr> </thead> <tbody> <tr> <td>11.1 CC</td> <td>This command was introduced.</td> </tr> </tbody> </table>	Release	Modification	11.1 CC	This command was introduced.			
Release	Modification							
11.1 CC	This command was introduced.							
Usage Guidelines	The aps lockdown command is configured only on protect interfaces.							
Examples	<p>The following example locks out (that is, prevents the circuit from switching to a protect interface in the event that the working circuit becomes unavailable) the POS interface 3/0/0:</p> <pre>router# configure terminal router(config)# interface pos 3/0/0 router(config-if)# aps protect 1 7.7.7.7 router(config-if)# aps lockdown 1 router(config-if)# end router#</pre>							
Related Commands	<table border="1"> <thead> <tr> <th>Command</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td>aps protect</td> <td>Enables a POS interface as a protect interface.</td> </tr> <tr> <td>aps working</td> <td>Configures a POS interface as a working interface.</td> </tr> </tbody> </table>	Command	Description	aps protect	Enables a POS interface as a protect interface.	aps working	Configures a POS interface as a working interface.	
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** interface configuration command. Use the **no** form of this command, to cancel the switch.

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	<table border="1"> <thead> <tr> <th style="border-top: 1px solid black; border-bottom: 1px solid black;">Release</th> <th style="border-top: 1px solid black; border-bottom: 1px solid black;">Modification</th> </tr> </thead> <tbody> <tr> <td style="border-bottom: 1px solid black;">11.1 CC</td> <td style="border-bottom: 1px solid black;">This command was introduced.</td> </tr> </tbody> </table>	Release	Modification	11.1 CC	This command was introduced.		
Release	Modification						
11.1 CC	This command was introduced.						
Usage Guidelines	<p>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.</p> <p>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.</p> <p>The aps manual command is a lower priority than any of the signal failures or the aps force command.</p>						
Examples	<p>The following example forces the circuit on POS interface 0 in slot 3 (a working interface) back onto the protect interface:</p> <pre>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#</pre>						
Related Commands	<table border="1"> <thead> <tr> <th style="border-top: 1px solid black; border-bottom: 1px solid black;">Command</th> <th style="border-top: 1px solid black; border-bottom: 1px solid black;">Description</th> </tr> </thead> <tbody> <tr> <td style="border-bottom: 1px solid black;">aps force</td> <td style="border-bottom: 1px solid black;">Manually switches the specified circuit to a protect interface, unless a request of equal or higher priority is in effect.</td> </tr> <tr> <td style="border-bottom: 1px solid black;">aps protect</td> <td style="border-bottom: 1px solid black;">Enables a POS interface as a protect interface.</td> </tr> </tbody> </table>	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 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** interface command. Use the **no** form of this command, to remove the POS interface as a protect interface.

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 due to a router failure, degradation or loss of channel signal, or manual intervention.



Note

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 7.7.7.7. 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 7.7.7.7
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** interface command. Use the **no** form of this command, to disable automatic switchover.

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	<table border="1"> <thead> <tr> <th style="border-top: 1px solid black; border-bottom: 1px solid black;">Release</th> <th style="border-top: 1px solid black; border-bottom: 1px solid black;">Modification</th> </tr> </thead> <tbody> <tr> <td style="border-bottom: 1px solid black;">11.1 CC</td> <td style="border-bottom: 1px solid black;">This command was introduced.</td> </tr> </tbody> </table>	Release	Modification	11.1 CC	This command was introduced.
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	<p>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:</p> <pre>router# configure terminal router(config)# interface pos 5/0/0 router(config-if)# aps protect 1 7.7.7.7 router(config-if)# aps revert 3 router(config-if)# end router#</pre>				
Related Commands	<table border="1"> <thead> <tr> <th style="border-top: 1px solid black; border-bottom: 1px solid black;">Command</th> <th style="border-top: 1px solid black; border-bottom: 1px solid black;">Description</th> </tr> </thead> <tbody> <tr> <td style="border-bottom: 1px solid black;">aps protect</td> <td style="border-bottom: 1px solid black;">Enables a POS interface as a protect interface.</td> </tr> </tbody> </table>	Command	Description	aps protect	Enables a POS interface as a protect interface.
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's router to be down, use the **aps timers** interface configuration command. Use the **no** form of this command, to return to the default timers.

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** interface configuration command. Use the **no** form of this command, to return to the default, bidirectional mode.

aps unidirectional

no aps unidirectional

Syntax Description This command has no arguments or keywords.

Defaults Bidirectional mode.

Command Modes Interface configuration

Release	Modification
11.1 CC	This command was introduced.

Usage Guidelines Use the **aps unidirectional** command when you must interoperate with SONET network equipment (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 POS interface as a working interface, use the **aps working** interface configuration command. Use the **no** form of this command, to remove the protect from the POS interface.

aps working *circuit-number*

no aps working *circuit-number*

Syntax Description	<i>circuit-number</i>	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** interface configuration command.



Note	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 the 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 PLIM, use the **atm sonet** interface configuration command. Use the **no** form of this command, to restore the default Synchronous Transport Signal level 12, concatenated (STS-12c) operation.

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

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, use the **auto-polarity** hub configuration command. Use the **no** form of this command to disable this feature.

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:

```
hub ethernet 0 1 3
  auto-polarity
```

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

bandwidth

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

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 and can be displayed with the EXEC command show interface .
-----------------	--

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

Command History	<table border="1"> <thead> <tr> <th>Release</th> <th>Modification</th> </tr> </thead> <tbody> <tr> <td>10.0</td> <td>This command was introduced.</td> </tr> </tbody> </table>	Release	Modification	10.0	This command was introduced.
Release	Modification				
10.0	This command was introduced.				

Usage Guidelines



Note

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

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.

IGRP uses the minimum path bandwidth to determine a routing metric. The TCP protocol adjusts initial retransmission parameters based on the apparent bandwidth of the outgoing interface.

At higher bandwidths, the value you configure with the **bandwidth** command is not what is displayed by the **show interface** command. The value shown is that used in IGRP updates and also used in computing load.



Note

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

Examples

The following example sets the full bandwidth for DS3 transmissions:

```
interface serial 0
bandwidth 44736
```

Related Commands

Command	Description
vines metric	Enables VINES routing on an interface.

cablelength

To specify the distance of the cable from the routers to the network equipment, use the **cablelength** controller configuration command. Use the **no** form of this command to restore the default cable length.

cablelength *feet*

no cablelength

Syntax Description	<i>feet</i>	Number of feet in the range of 0 to 450. The default varies for different routers.
---------------------------	-------------	--

Defaults	224 feet for CT3IP interface processor. 50 feet for PA-T3 and PA-2T3 port adapters.
-----------------	--

Command Modes	Controller configuration
----------------------	--------------------------

Command History	Release	Modification
	11.1 CA	This command was introduced.

Usage Guidelines	<p>If you do not specify the cablelength command, the default cable length of 224 feet is used by the CT3IP.</p> <p>If you do not specify the cablelength command, the default cable length of 50 feet is used by the PA-T3 and PA-2T3.</p>
-------------------------	---



Note

Although you can specify a cable length from 0 to 450 feet, the hardware only recognizes two ranges: 0 to 224 and 225 to 450. For example, entering 150 feet uses the 0 to 224 range. If you later change the cable length to 200 feet, there is no change because 200 is within the 0 to 224 range. However, if you change the cable length to 250, the 225 to 450 range is used. The actual number you enter is stored in the configuration file.

Examples	The following example sets the cable length for the router to 300:
-----------------	--

```
controller t3 9/0/0
cablelength 300
```

cablelength long

To increase the pulse of a signal at the receiver and decrease the pulse from the transmitter using pulse equalization and line build-out for a T1 cable on a Cisco AS5200, use the **cablelength long** controller configuration command. Use the **no** form of this command, to return the pulse equalization and line build-out values to their default settings.

cablelength long *dbgain-value dbloss-value*

no cablelength long

Syntax Description	<i>dbgain-value</i>	Number of decibels by which the receiver signal is increased. Use one of the following keywords to specify this value: <ul style="list-style-type: none"> • gain26 • gain36
	<i>dbloss-value</i>	Number of decibels by which the transmit signal is decreased. Use one of the following keywords to specify this value: <ul style="list-style-type: none"> • 0db • -7.5db • -15db • -22.5db

Defaults Gain of 26 dB, and transmitter loss of 0 dB.

Command Modes Controller configuration

Command History	Release	Modification
	11.2	This command was introduced.
	11.3	The following choices were added: gain26 , gain36 , -15db , -22.5db , -7.5db , and 0db .

Usage Guidelines Use this command for configuring the controller T1 interface on the AS5200 access server or on the Cisco MC3810 multiservice access concentrator, the **cablelength long** command is used to configure DS1 links (meaning, to build CSU/DSU links) when the cable length is no longer than 655 feet. On the Cisco MC3810, this command is supported on T1 controllers only.

On the Cisco MC3810, this command applies to Voice over Frame Relay, Voice over ATM, and Voice over HDLC.



Note On the Cisco MC3810, you cannot use the **cablelength long** command on a DSX-1 interface only. The **cablelength long** command can be only used on CSU interfaces.

A pulse equalizer regenerates a signal that has been attenuated and filtered by a cable loss. Pulse equalization does not produce a simple gain, but it filters the signal to compensate for complex cable loss. A **gain26** receiver gain compensates for a long cable length equivalent to 26 dB of loss, while a **gain36** compensates for 36 dB of loss.

The lengthening or *building out* of a line is used to control far-end crosstalk. Line build-out attenuates the stronger signal from the customer installation transmitter so that the transmitting and receiving signals have similar amplitudes. A signal difference of less than 7.5 dB is ideal. Line build-out does not produce simple flat loss (also known as *resistive* flat loss). Instead, it simulates a cable loss of 7.5 dB, 15 dB, or 22.5 dB so that the resulting signal is handled properly by the receiving equalizer at the other end.

Examples

The following example increases the receiver gain by 26 decibels and decreases the transmitting pulse by 7.5 decibels for a long cable:

```
AS5200(config)# controller t1 0
AS5200(config-controller)# cablelength long gain26 -7.5db
```

The following example configures the cable length for controller T1 0 on a Cisco MC3810 to a decibel pulse gain of 36 and a decibel pulse rate of -22.5 decibels:

```
MC3810(config)# controller t1 0
MC3810(config)# cablelength long gain36 -22.5db
```

Related Commands

Command	Description
cablelength short	Sets a cable length 655 feet or shorter for a DS1 link on the Cisco MC3810 multiservice concentrator.

cablelength short

To set a cable length 655 feet or shorter for a DS1 link on the Cisco MC3810, use the **cablelength short** controller configuration command. This command is supported on T1 controllers only. The **no** form of this command deletes the **cablelength short** value. To set cable lengths longer than 655 feet, use the **cablelength long** command.

cablelength short { **133** | **266** | **399** | **533** | **655** }

no cablelength short

Syntax Description		
	133	Specifies a cable length from 0-133 feet.
	266	Specifies a cable length from 134-266 feet.
	399	Specifies a cable length from 267-399 feet.
	533	Specifies a cable length from 400-533 feet.
	655	Specifies a cable length from 534-655 feet.

Defaults 133 feet

Command Modes Controller configuration mode

Command History	Release	Modification
	11.3(2)AA	This command was introduced.

Usage Guidelines On the Cisco MC3810, the **cablelength short** command is used to configure DSX-1 links when the cable length is 655 feet or less than 655 feet. On the Cisco MC3810, this command is supported on T1 controllers only.



Note

On the Cisco MC3810, you cannot enter the **cablelength short** command on a CSU interface. The **cablelength short** command can only be used on DSX-1 interfaces.

Examples In the following example, the cable length is set to 266 for the T1 controller in slot 0 on dial shelf 0:

```
router# configure terminal
router(config)# controller t1 1/1/0
router(config-controller)# cablelength short 266
router (config-controller)# exit
router(config)# exit
router#
```

Related Commands

Command	Description
cablelength long	Increases the pulse of a signal at the receiver and decreases the pulse from the sender using pulse equalization and line build-out for a T1 cable on a Cisco AS5200 access server.

carrier-delay

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

carrier-delay [*seconds*]

no carrier-delay [*seconds*]

Syntax Description	<i>seconds</i>	Time, in seconds, to wait for the system to change states. Enter an integer in the range 0 to 60. The default is 2 seconds.
---------------------------	----------------	---

Defaults The default carrier delay is 2 seconds.

Command Modes Interface configuration

Command History	Release	Modification
	10.1	This command was introduced.

Usage Guidelines Carrier delay works like this: 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 you choose depends on the nature of the link outages you expect to see in your network, and how long you expect those outages to last.

If your data links 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.

However, if your outages tend to be longer, then you may 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
```

cas-group

To configure channelized T1 time slots with channel associated signaling (also known as *robbed bit signaling*), which enables a Cisco AS5200 modem to answer and send an analog call, use the **cas-group** controller configuration command. Use the **no** form of this command to disable channel associated signaling for one or more timeslots.

cas-group *channel-number* [**timeslots** *range*]

no cas-group *channel-number* [**timeslots** *range*]

Syntax Description		
	<i>channel-number</i>	Specifies a single channel group number. The channel number can be between 0 and 23.
	timeslots <i>range</i>	(Optional) Specifies a timeslot range of values from 1 to 24. The default value configures 24 timeslots with the channel associated signal called E&M (Ear and Mouth), which is the default signal type.

Defaults Disabled

Command Modes Controller configuration

Command History	Release	Modification
	11.2	This command was introduced.

Usage Guidelines Use this command to enable a Cisco AS5200 modem to receive and send incoming and outgoing analog calls through each T1 controller that is configured for a channelized T1 line, which has 24 possible channels.

Switched 56 digital calls are not supported under this new feature.

Examples

The following example configures all 24 channels to support robbed bit signaling on a Cisco AS5200:


```
AS5200(config)# controller T1 0
AS5200(config-controller)# cas-group 1 timeslots 1-24
AS5200(config-controller)#
%D SX0-5-RBSLINEUP: RBS of controller 1 timeslot 1 is up
%D SX0-5-RBSLINEUP: RBS of controller 1 timeslot 2 is up
%D SX0-5-RBSLINEUP: RBS of controller 1 timeslot 3 is up
%D SX0-5-RBSLINEUP: RBS of controller 1 timeslot 4 is up
%D SX0-5-RBSLINEUP: RBS of controller 1 timeslot 5 is up
%D SX0-5-RBSLINEUP: RBS of controller 1 timeslot 6 is up
%D SX0-5-RBSLINEUP: RBS of controller 1 timeslot 7 is up
%D SX0-5-RBSLINEUP: RBS of controller 1 timeslot 8 is up
%D SX0-5-RBSLINEUP: RBS of controller 1 timeslot 9 is up
%D SX0-5-RBSLINEUP: RBS of controller 1 timeslot 10 is up
%D SX0-5-RBSLINEUP: RBS of controller 1 timeslot 11 is up
%D SX0-5-RBSLINEUP: RBS of controller 1 timeslot 12 is up
%D SX0-5-RBSLINEUP: RBS of controller 1 timeslot 13 is up
%D SX0-5-RBSLINEUP: RBS of controller 1 timeslot 14 is up
%D SX0-5-RBSLINEUP: RBS of controller 1 timeslot 15 is up
%D SX0-5-RBSLINEUP: RBS of controller 1 timeslot 16 is up
%D SX0-5-RBSLINEUP: RBS of controller 1 timeslot 17 is up
%D SX0-5-RBSLINEUP: RBS of controller 1 timeslot 18 is up
%D SX0-5-RBSLINEUP: RBS of controller 1 timeslot 19 is up
%D SX0-5-RBSLINEUP: RBS of controller 1 timeslot 20 is up
%D SX0-5-RBSLINEUP: RBS of controller 1 timeslot 21 is up
%D SX0-5-RBSLINEUP: RBS of controller 1 timeslot 22 is up
%D SX0-5-RBSLINEUP: RBS of controller 1 timeslot 23 is up
%D SX0-5-RBSLINEUP: RBS of controller 1 timeslot 24 is up
```

channel-group (Fast EtherChannel)

To assign a Fast Ethernet interface to a Fast EtherChannel group, use the **channel-group** interface configuration command. 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	<i>channel-number</i> 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 assigned.				
Command Modes	Interface configuration				
Command History	<table border="1"> <thead> <tr> <th style="border-top: 1px solid black; border-bottom: 1px solid black;">Release</th> <th style="border-top: 1px solid black; border-bottom: 1px solid black;">Modification</th> </tr> </thead> <tbody> <tr> <td style="border-bottom: 1px solid black;">11.1 CA</td> <td style="border-bottom: 1px solid black;">This command was introduced.</td> </tr> </tbody> </table>	Release	Modification	11.1 CA	This command was introduced.
Release	Modification				
11.1 CA	This command was introduced.				
Usage Guidelines	<p>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.</p> <p>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 interface configuration command.</p> <p>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 RSP700CI and a Catalyst 5000 switch.</p> <p>Up to four Fast Ethernet interfaces can be added to a Fast EtherChannel group.</p>				
 Caution	<p>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.</p>				
	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
Router(config-if)# channel-group 1
```

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 controller lex

To reboot the LAN Extender chassis and restart its operating software, use the **clear controller lex** privileged EXEC command.

clear controller lex *number* [**prom**]

Cisco 7500 Series

clear controller lex *slot/port* [**prom**]

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

clear controller lex [*type slot/port*]

Cisco 7500 Series with Ports on VIP Cards

clear controller lex [*type slot/port-adapter/port*]

Syntax Description		
	<i>number</i>	Number of the LAN Extender interface corresponding to the LAN Extender to be rebooted.
	prom	(Optional) Forces a reload of the PROM image, regardless of any Flash image.
	<i>slot</i>	Refer to the appropriate hardware manual for slot and port information.
	<i>port</i>	Refer to the appropriate hardware manual for slot and port information.
	<i>type</i>	(Optional) Specifies the interface type. See Table 1 for keywords.
	<i>port-adapter</i>	Refer to the appropriate hardware manual for information about port adapter compatibility.

Command Modes Privileged EXEC

Command History	Release	Modification
	10.3	This command was introduced.

Usage Guidelines The **clear controller lex** command halts operation of the LAN Extender and performs a cold restart. Without the **prom** keyword, if an image exists in Flash memory, and that image has a newer software version than the PROM image, and that image has a valid checksum, then this command runs the Flash image. If any one of these three conditions is not met, this command reloads the PROM image. With the **prom** keyword, this command reloads the PROM image, regardless of any Flash image.

Examples

The following example halts operation of the LAN Extender bound to LAN Extender interface 2 and causes the LAN Extender to perform a cold restart from Flash memory:

```
Router# clear controller lex 2  
reload remote lex controller? [confirm] yes
```

The following example halts operation of the LAN Extender bound to LAN Extender interface 2 and causes the LAN Extender to perform a cold restart from PROM:

```
Router# clear controller lex 2 prom  
reload remote lex controller? [confirm] yes
```

clear counters

To clear the interface counters, use the **clear counters** EXEC command.

clear counters [*type number*]

Cisco 4000 Series or Cisco 7500 Series with a LAN Extender Interface

clear counters [*type slot/port*] [**ethernet** | **serial**]

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	<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.
	ethernet	(Optional) If the <i>type</i> is lex , you can clear the interface counters on the Ethernet interface.
	serial	(Optional) If the <i>type</i> is lex , you can clear the interface counters on the serial interface.
	<i>slot</i>	Refer to the appropriate hardware manual for slot and port information.
	<i>port</i>	Refer to the appropriate hardware manual for slot and port information.
	<i>port-adapter</i>	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.
	11.3	The following keywords were added or modified: <ul style="list-style-type: none"> • vg-anylan • posi keyword was changed to pos.

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 will not clear counters retrieved using 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	Integrated Services Digital Network (ISDN) Basic Rate Interface (BRI)
dialer	Dialer interface
ethernet	Ethernet interface
fast-ethernet	Fast Ethernet interface
fdi	Fiber Distributed Data Interface (FDDI)
hssi	High-Speed Serial Interface (HSSI)
lex	LAN Extender interface
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
vg-anylan	100VG-AnyLAN port adapter

Examples

The following example clears all interface counters:

```
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:

```
clear counters pos 1/0
```

The following example clears interface counters on the serial interface residing on a Cisco 1000 series LAN Extender:

```
clear counters lex 0 serial
```

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]
%CLEAR-5-COUNTERS: Clear counter on all interfaces by console 1
```

Related Commands

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

Use the **clear hub** EXEC command to reset and reinitialize the hub hardware connected to an interface of a Cisco 2505 or Cisco 2507 router.

clear hub ethernet *number*

Syntax Description	ethernet	Indicates the hub in front of an Ethernet interface.
	<i>number</i>	Hub number to clear, starting with 0. Since there is currently 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:

```
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.

clear hub counters

Use the **clear hub counters** EXEC command to set to zero the hub counters on an interface of a Cisco 2505 or Cisco 2507 router.

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

Syntax Description	Parameter	Description
	ether	(Optional) Indicates the hub in front of an Ethernet interface.
	<i>number</i>	(Optional) Hub number for which to clear counters. Since 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, then 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 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:

```
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

Use the **clear interface** EXEC command to reset the hardware logic on an interface.

clear interface *type number*

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>	Specifies the interface type; it is one of the keywords listed in Table 1 in the “Usage Guidelines” section.
	<i>number</i>	Specifies the port, connector, or interface card number.
	<i>slot</i>	Refer to the appropriate hardware manual for slot and port information.
	<i>port</i>	Refer to the appropriate hardware manual for slot and port information.
	<i>port-adapter</i>	Refer to the appropriate hardware manual for information about port adapter compatibility.
	: <i>channel-group</i>	(Optional) On Cisco 7500 series routers supporting channelized T1, specifies the channel 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 • posi keyword was changed to pos.

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 optional arguments *type* and *number* 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	Asynchronous Transfer Mode (ATM) interface
bri	Integrated Services Digital Network (ISDN) Basic Rate Interface (BRI)
ethernet	Ethernet interface
fddi	Fiber Distributed Data Interface (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:

```
clear interface hssi 1
```

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

```
clear interface pos 1/0
```

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

```
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
```

clear interface fastethernet

Use the **clear interface fastethernet** privileged EXEC command to reset the controller for a specified Fast Ethernet interface.

Cisco 4500 and 4700 series

```
clear interface fastethernet number
```

Cisco 7200 and 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 NPM number. The numbers are assigned at the factory at the time of installation or when added to a system.
	<i>slot</i>	Refer to the appropriate hardware manual for slot and port information.
	<i>port</i>	Refer to the appropriate hardware manual for slot and port information.
	<i>port-adapter</i>	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

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

```
clear interface fastethernet 0
```

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

```
clear interface fastethernet 1/0
```

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

```
clear interface fastethernet 1/0/0
```

clear rif-cache

Use the **clear rif-cache** EXEC command to clear entries from the Routing Information Field (RIF) cache.

clear rif-cache

Syntax Description This command has no arguments or keywords.

Command Modes EXEC

Command History	Release	Modification
	10.0	This command was introduced.

Examples The following example clears the RIF cache:

```
clear rif-cache
```

Related Commands	Command	Description
	multiring	Enables collection and use of RIF information.

clear service-module serial

Use the **clear service-module serial** privileged EXEC configuration command to reset an integrated CSU/DSU.

clear service-module serial *number*

Syntax Description	<i>number</i>	Number of the serial interface.
---------------------------	---------------	---------------------------------

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

Command History	Release	Modification
	11.2	This command was introduced.

Usage Guidelines Use this command only in severe circumstances (for example, when the router is not responding to a CSU/DSU configuration command).

This command terminates all DTE and line loopbacks that are locally or remotely configured. It also interrupts data transmission through the router for up to 15 seconds. The software performs an automatic software reset in case of two consecutive configuration failures.

The CSU/DSU module is not reset with the **clear interface** command.



Caution

If you experience technical difficulties with your router and intend to contact customer support, refrain from using this command. This command erases the router's past CSU/DSU performance statistics. To clear only the CSU/DSU performance statistics, issue the **clear counters** command.

Examples

The following example resets the CSU/DSU on a router:

```
router# clear service-module serial 0
router#
```

Related Commands	Command	Description
	clear counters	Clears the interface counters.
	test service-module	Performs self-tests on an integrated CSU/DSU serial interface module, such as a 4-wire, 56/64-kbps CSU/DSU.

clock rate

Use the **clock rate** interface configuration command to configure the clock rate for the hardware connections on serial interfaces such as network interface modules (NIMs) and interface processors to an acceptable bit rate. Use the **no** form of this command to remove the clock rate if you change the interface from a DCE to a DTE device. Using the **no** form of this command on a DCE interface sets the clock rate to the hardware-dependent default value.

clock rate *bps*

no clock rate

Syntax Description

bps Desired clock rate in bits per second: 1200 2400 4800 9600 19200 38400 56000 64000 72000 125000 148000 250000 500000 800000 1000000 1300000 2000000 4000000 or 8000000.

For the synchronous serial port adapters (PA-8T-V35, PA-8T-X21, PA-8T-232, and PA-4T+), a nonstandard clock rate can be used. You can enter any value from 300 to 8000000 bps. The clock rate you enter is rounded (adjusted), if necessary, to the nearest value your hardware can support except for the following standard rates: 1200 2400 4800 9600 14400 19200 28800 38400 56000 64000 128000 or 2015232.

Defaults

No clock rate is configured.

Command Modes

Interface configuration

Command History

Release	Modification
10.0	This command was introduced.
11.3	This command was modified to include nonstandard clock rates for the PA-8T-V35, PA-8T-X21, PA-8T-232, and PA-4T+ synchronous serial port adapters.

Usage Guidelines

Cable Length

Be aware that the fastest speeds might not work if your cable is too long, and that speeds faster than 148,000 bits per second are too fast for EIA/TIA-232 signaling. It is recommended that you only use the synchronous serial EIA/TIA-232 signal at speeds up to 64,000 bits per second. To permit a faster speed, use EIA/TIA-449 or V.35.

Synchronous Serial Port Adapters

For the synchronous serial port adapters (PA-8T-V35, PA-8T-X21, PA-8T-232, and PA-4T+) on Cisco 7200 series routers, and on second-generation Versatile Interface Processors (VIP2s) in Cisco 7500 series routers, the clock rate you enter is rounded (if needed) to the nearest value that your hardware can support. To display the clock rate value for the port adapter, use the **more system:running-config** command.

If you plan to netboot your router over a synchronous serial port adapter interface and have a boot image prior to Cisco IOS Release 11.1(9)CA that does not support nonstandard (rounded) clock rates for the port adapters, you must use one of the following standard clock rates:

1200, 2400, 4800, 9600, 19200, 38400, 56000, 64000

Examples

The following example sets the clock rate on the first serial interface to 64,000 bits per second:

```
interface serial 0
  clock rate 64000
```

The following example sets the clock rate on a synchronous serial port adapter in slot 5, port 0 to 1234567. In this example, the clock rate is adjusted to 1151526 bps.

```
interface serial 5/0
  clock rate 1234567
%Clockrate rounded to nearest value that your hardware can support.
%Use Exec Command 'more system:running-config' to see the value rounded to.
```

The following example configures serial interface 5/0 with a clock rate that is rounded to the nearest value that is supported by the hardware:

```
Router# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)# interface serial 5/0
Router(config-if)# clock rate 1234567
%Clockrate rounded to nearest value that your hardware can support.
%Use Exec Command 'more system:running-config' to see the value rounded to.
Router(config-if)# exit
Router(config)#
```

The following example shows how to determine the exact clock rate that the serial interface was rounded to using the **more system:running-config** command. This example shows only the relevant information displayed by the **more system:running-config** command; other information was omitted.

```
Router# more system:running-config
Building configuration...
...
!
interface Serial5/0
  no ip address
  clockrate 1151526
!
...
```

clock source (CT3IP)

Use the **clock source** controller configuration command to specify where the clock source is obtained for use by the Channelized T3 Interface Processor (CT3IP) in Cisco 7500 series routers. Use the **no** form of this command to restore the default clock source.

clock source { **internal** | **line** | **loop-timed** }

no clock source

Syntax Description

internal	Specifies that the internal clock source is used. This is the default.
line	Specifies that the network clock source is used.
loop-timed	Decouples the controller clock from the system-wide clock set with the network-clock-select command. The loop-timed clock enables the DVM to connect to a PBX and to connect the MFT to a central office when both the PBX and the central office function as DCE clock sources. This situation assumes that the PBX also takes the clocking from the central office thereby synchronizing the clocks on the DVM and the MFT.

Defaults

Internal

Command Modes

Controller configuration

Command History

Release	Modification
11.3	This command was introduced.

Usage Guidelines

If you do not specify the **clock source** command, the default clock source of internal is used by the CT3IP.

You can also set the clock source for each T1 channel by using the **t1 clock source** controller configuration command.



Note

This command replaces the **pos internal-clock** command.

Examples

The following example sets the clock source for the CT3IP to line:

```
controller t3 9/0/0
clock source line
```

■ clock source (CT3IP)

Related Commands	Command	Description
	t1 clock source	Specifies where the clock source is obtained for use by each T1 channel on the CT3IP in Cisco 7500 series routers.

clock source (Cisco AS5200)

Use the **clock source** interface configuration command to select the clock source for the time-division multiplexing (TDM) bus in a Cisco AS5200 access server. The **no** form of this command configures the clock source to its default setting.

clock source {line {primary | secondary} | internal}

no clock source line {primary | secondary}

Syntax Description	line	Clock source on the active line.
	primary	Primary TDM clock source.
	secondary	Secondary TDM clock source.
	internal	Selects the free running clock (also known as internal clock) as the clock source.

Defaults	Primary TDM clock source from the T1 0 controller Secondary TDM clock source from the T1 1 controller
----------	--

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

Command History	Release	Modification
	11.2	This command was introduced.

Usage Guidelines	To use the clocking coming in from a T1 line, configure the clock source line primary command on the T1 interface that has the most reliable clocking. Configure the clock source line secondary command on the T1 interface that has the next best known clocking. With this configuration, the primary line clocking is backed up to the secondary line if the primary clocking shuts down.
------------------	---

Examples	The following example configures the Cisco AS5200 access server to use T1 controller 0 as the primary clock source and T1 controller 1 as the secondary clock source:
----------	---

```
controller t1 0
clock source line primary
controller t1 1
clock source line secondary
```

clock source (Cisco MC3810)

To specify the clock source of a DS1 link on the Cisco MC3810, use the **clock source** controller configuration command .

clock source { line | internal | loop-timed }

Syntax Description

line	Specifies that the DS1 link uses the recovered clock. The line value is the default clock source used when the Multiflex Trunk (MFT) is installed.
internal	Specifies that the DS1 link uses the internal clock. The internal value is the default clock source used when the Digital Voice Module (DVM) is installed.
loop-timed	Specifies that the T1/E1 controller will take the clock from the Rx (line) and use it for Tx. This setting decouples the controller clock from the system-wide clock set with the network-clock-select command. The loop-timed clock enables the DVM to connect to a PBX and to connect the MFT to a central office when both the PBX and the central office function as DCE clock sources. This situation assumes that the PBX also takes the clocking from the central office thereby synchronizing the clocks on the DVM and the MFT.

Defaults

Line (when the MFT is installed)
Internal (when the DVM is installed)

Command Modes

Controller configuration mode

Command History

Release	Modification
11.1	This command was introduced.

Usage Guidelines

This command applies to Voice over Frame Relay, Voice over ATM, and Voice over HDLC on the Cisco MC3810.

Examples

The following example configures the clock source for the MFT to internal, and the clock source for the DVM for line on a Cisco MC3810:

```
controller T1 0
  clock source internal

controller T1 1
  clock source line
```



Note

You cannot configure the clock source to the line setting for both T1/E1 controllers at the same time.

clock source (controller)

Use the **clock source** controller configuration command to set the T1-line clock-source for the MIP in the Cisco 7200 series and Cisco 7500 series or for the NPM in the Cisco 4000 series or a T3 interface or a PA-T3 serial port adapter.

clock source {line | internal}

Syntax Description	internal	line
	Specifies that the interface will clock its transmitted data from its internal clock.	Specifies that the interface will clock its transmitted data from a clock recovered from the line's receive data stream (default).

Defaults	<p>Primary TDM clock source from the T0 controller</p> <p>Secondary TDM clock source from the T1 controller</p> <p>The line's receive data stream from the PA-T3 serial port adapter</p>
----------	--

Command Modes	Controller configuration
---------------	--------------------------

Command History	Release	Modification
	10.3	This command was introduced.
	11.1 CA	This command was modified to include the T3 serial port adapter and PA-T3 serial port adapter.

Usage Guidelines	<p>This command applies to a Cisco 4000 router or Cisco 7000 series, Cisco 7200 series, and Cisco 7500 series router. A T3 interface on a PA-T3 serial port adapter can clock its transmitted data from either its internal clock or from a clock recovered from the line's receive data stream.</p>
------------------	--

To use the clocking coming in from a T1 line, configure the **clock source line primary** command on the controller that has the most reliable clocking. Configure the **clock source line secondary** command on the controller that has the next best known clocking. With this configuration, the primary line clocking is backed up to the secondary line if the primary clocking shuts down.

Examples	<p>The following example configures the Cisco AS5200 to use the T0 controller as the primary clocking source and the T1 controller as the secondary clocking source:</p>
----------	--

```
AS5200(config)# controller t1 0
AS5200(config-if)# clock source line primary
AS5200(config-if)# exit
AS5200(config)# controller t1 1
AS5200(config-if)# clock source line secondary
```

The following example specifies the T3 interface to clock its transmitted data from its internal clock:

```
interface serial 1/0
 clock source internal
```

Related Commands	Command	Description
	framing (E1/T1 controller)	Selects the frame type for the T1 or E1 data line.
	linecode	Selects the linecode type for T1 or E1 line.

clock source (interface)

To control the clock used by a G.703-E1 interface, an E1-G.703/G.704 serial port adapter, or a PA-E3 serial port adapter will use to clock its transmitted data from, use the **clock source** interface configuration command. Use the **no** form of this command, to restore the default value.

Cisco 4000, 7000, 7200, and 7500 Series

clock source { **line** | **internal** }

no clock source

Cisco AS5200 and AS5300 Access Servers

clock source { **line** { **primary** | **secondary** } | **internal** }

no clock source line { **primary** | **secondary** }

Syntax Description

line	Specifies that the interface will clock its transmitted data from a clock recovered from the line's receive data stream (default).
internal	Specifies that the interface will clock its transmitted data from its internal clock.
primary	Primary TDM clock source.
secondary	Secondary TDM clock source.

Defaults

Cisco 4000, 7000, 7200, and 7500 Series

The clock source is the line's receive data stream.

Cisco AS5200 and AS5300 Access Servers

Primary TDM clock source from the T0 controller

Secondary TDM clock source from the T1 controller

Command Modes

Interface configuration

Command History

Release	Modification
10.3	This command was introduced for the Cisco 4000 series, Cisco 7000 series with RSP7000, and Cisco 7500 series with the G.703 E1 interface.
11.1 CA	This command was introduced for the time-division multiplexing (TDM) bus in a Cisco AS5200 and Cisco AS5300 access server.
11.1 CA	This command was modified to include the E1-G.703/G.704 serial port adapter, PA-E3 serial port adapters, and Cisco 7200 series routers.

Usage Guidelines**Cisco 4000, 7000, 7200, and 7500 Series**

A G.703-E1 interface, E1-G.703/G.704 serial port adapter, or a PA-E3 serial port adapter can clock its transmitted data from either its internal clock or from a clock recovered from the line's receive data stream.

Cisco AS5200 and AS5300 Access Servers

To use the clocking coming in from a T1 line, configure the **clock source line primary** command on the controller that has the most reliable clocking. Configure the **clock source line secondary** command on the controller that has the next best known clocking. With this configuration, the primary line clocking is backed up to the secondary line if the primary clocking shuts down.

Examples**Cisco 4000, 7000, 7200, and 7500 Series**

The following example specifies the G.703-E1 interface to clock its transmitted data from its internal clock:

```
interface serial 0/1
clock source internal
```

Cisco AS5200 and AS5300 Access Servers

The following example configures the Cisco AS5200 to use the T0 controller as the primary clocking source and the T1 controller as the secondary clocking source:

```
AS5200(config)# controller t1 0
AS5200(config-if)# clock source line primary
AS5200(config-if)# exit
AS5200(config)# controller t1 1
AS5200(config-if)# clock source line secondary
```

cmt connect

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

cmt connect [*interface-name* **phy-a** | **phy-b**]

Syntax Description	
<i>interface-name</i>	(Optional) Specifies the FDDI interface.
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.

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:

```
cmt connect
```

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

```
cmt connect fddi 0
```

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

```
cmt connect fddi 1/0
```

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

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

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

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

cmt disconnect

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

cmt disconnect [*interface-name* [**phy-a** | **phy-b**]]

Syntax Description	<i>interface-name</i> (Optional) Specifies the FDDI interface.
	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** interface configuration command. 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.

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:

```
cmt disconnect
```

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

```
cmt disconnect fddi 0
```

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

```
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.

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

The following command on the Cisco 7500 series stops only Physical Sublayer A on the 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.

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

compress

To configure software compression for Link Access Procedure, Balanced (LAPB), Point-to-Point Protocol (PPP), and High-Level Data Link Control (HDLC) encapsulations, use the **compress** interface configuration command. 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]}
```

Cisco 7200 Series

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

PPP Encapsulation

```
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	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 VIP2, compression is implemented in the software installed in the router's main processor. On Cisco 7200 series, 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: <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 the CSA is not available, compression is performed in the software installed on the VIP2 (distributed compression). • If the 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. This option applies only to Cisco 7200 series routers.	

mppc	(Optional) Specifies that the MPPC compression algorithm will 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

Release	Modification
10.0	The compress predictor command was introduced.
10.3	The compress predictor command was changed to the compress command, and the following keywords were added: <ul style="list-style-type: none"> • predictor • stac
11.3 P	The following keywords were added: <ul style="list-style-type: none"> • distributed • software • csa
11.3 T	The following keywords were added: <ul style="list-style-type: none"> • mppc • ignore-pfc

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

Compression reduces the size of frames via lossless data compression. You can configure point-to-point software compression for all LAPB, PPP, and HDLC encapsulations. HDLC encapsulations supports the Stacker compression algorithm. PPP and LAPB encapsulations support both predictor and Stacker compression algorithms.

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.

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 uncompressed standard protocol field value for IP is 0x0021 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 which 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.

Point-to-Point Compression

You can configure point-to-point software compression for all LAPB, PPP, and HDLC encapsulations. Compression reduces the size of frames via lossless data compression. 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.

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

When compression is performed in software installed in the router's main processor, it might significantly affect system performance. 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
The bottleneck is caused by the load on the router.	Predictor
The 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 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 or one 256-kbps line. These maximums also assume 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 *Wide-Area Networking Configuration Guide*.

Examples

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

```
interface serial 3/1/0
 encapsulate ppp
 compress stac
```

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

```
interface serial 0
 encapsulation lapb
 compress predictor
 mtu 1509
 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:

```
interface serial 0
 encapsulation lapb
 compress predictor
```

The following example configures BRI interface 0 to perform MPPC:

```
interface BRI0
 ip unnumbered ethernet0
 encapsulation ppp
 isdn spid1 5551234
 dialer map ip 172.21.71.74 5551234
 dialer-group 1
 compress mppc
```

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

```
interface async1
 ip unnumbered ethernet0
 encapsulation ppp
 async default routing
 async dynamic routing
 async mode interactive
 peer default ip address 172.21.71.74
 compress mppc ignore-pfc
```

Related Commands

Command	Description
encapsulation	Sets encapsulation method used by the interface (see lapb and ppp keywords).
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.

controller t3

To configure the Channelized T3 Interface Processor (CT3IP) in Cisco 7500 series routers, use the **controller t3** global configuration command.

controller t3 *slot/port-adapter/port*

Syntax Description	<i>slot</i>	Refer to the appropriate hardware manual for slot and port information.
	<i>port</i>	Refer to the appropriate hardware manual for slot and port information.
	<i>port-adapter</i>	Refer to the appropriate hardware manual for information about port adapter compatibility.
Defaults	No T3 controller is configured.	
Command Modes	Global configuration	
Command History	Release	Modification
	11.3	This command was introduced.
Usage Guidelines	This command is used to configure the CT3IP and the 28 T1 channels. After the T1 channels are configured, continue to configure each T1 channel as a serial interface by using the interface serial global configuration command.	
Examples	The following example configures the CT3IP in slot 3:	
	<pre>controller t3 3/0/0</pre>	
Related Commands	Command	Description
	interface serial	Specifies a serial interface created on a channelized E1 or channelized T1 controller (for ISDN PRI, CAS, or robbed bit signalling).

copy flash lex

To download an executable image from Flash memory on the core router to the LAN Extender chassis, use the **copy flash lex** privileged EXEC command.

copy flash lex *number*

Syntax Description

<i>number</i>	Number of the LAN Extender interface to which to download an image from Flash memory.
---------------	---

Command Modes

Privileged EXEC

Command History

Release	Modification
10.3	This command was introduced.

Usage Guidelines

If you attempt to download a version of the software older than what is currently running on the LAN Extender, a warning message is displayed.

Examples

The following example copies the executable image *namexx* to the LAN Extender interface 0:

```
Router# copy flash lex 0
Name of file to copy? namexx
Address of remote host [255.255.255.255] <cr>
writing namexx !!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!copy complete
```

Related Commands

Command	Description
copy tftp lex	Downloads an executable image from a TFTP server to the LAN Extender chassis.

copy tftp lex

To download an executable image from a TFTP server to the LAN Extender, use the **copy tftp lex** privileged EXEC command.

copy tftp lex *number*

Syntax Description	<i>number</i>	Number of the LAN Extender interface to which to download an image.
---------------------------	---------------	---

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

Command History	Release	Modification
	10.3	This command was introduced.

Usage Guidelines	If you attempt to download a version of the software older than what is currently running on the LAN Extender, a warning message is displayed.
-------------------------	--

Examples The following example copies the file *namexx* from the TFTP server:

```
Router# copy tftp lex 0
Address or name of remote host (255.255.255.255)? 131.108.1.111
Name of file to copy? namexx
OK to overwrite software version 1.0 with 1.1 ?[confirm]
Loading namexx from 131.108.13.111!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
[OK - 127825/131072 bytes]

Successful download to LAN Extender
```

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** interface configuration command. 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).
---------------------------	---------------------------------------

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 cyclic redundancy check (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>
-------------------------	--

CRC-16, the most widely used throughout the United States and Europe, is used extensively with wide-area networks (WANs). CRC-32 is specified by IEEE 802 and as an option by some point-to-point transmission standards. It is often used on SMDS networks and LANs.

Examples	The following example enables the 32-bit CRC on serial interface 3/0:
-----------------	---

```
interface serial 3/0
  crc 32
```

crc4

To enable generation of CRC4 (per ITU Recommendation G.704 and G.703) to improve data integrity, use the **crc4** interface configuration command. 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, Cisco 7200 series, Cisco 7000 series, and Cisco 7500 series router. This command is supported on the 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 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:

```
interface Serial 0/0
  crc 32
  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** interface configuration command. 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 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 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 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:

```
interface Serial 0/0
  crc 32
  crc bits 5
```

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** interface command. 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

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 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 off-loads 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 system:running-config	Displays the running configuration.