

storm-control

To set the storm-control threshold value and block forwarding of unnecessary flooded traffic, use the **storm-control** command in interface configuration mode. To turn off storm control and restore the default threshold, use the **no** form of this command.

storm-control { **broadcast** *threshold* | **multicast** *threshold* | **unicast** *threshold* }

no storm-control

Syntax Description

broadcast	Specifies the broadcast suppression level for an interface as a percentage of total bandwidth.
multicast	Specifies the multicast suppression level for an interface as a percentage of total bandwidth.
unicast	Specifies the unicast suppression level for an interface as a percentage of total bandwidth.
<i>threshold</i>	Specifies the limit (percentage) placed on broadcast traffic: A threshold value of 100 percent means that no limit is placed on broadcast traffic. Valid entries are from 1 to 100.

Defaults

The **storm-control** command is disabled and the threshold value is 100 percent.

Command Modes

Interface configuration

Command History

Release	Modification
12.2(2)XT	This command was introduced on the Cisco 2600 series, the Cisco 3600 series, and the Cisco 3700 series routers.
12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T to support switchport creation on Cisco 2600 series, the Cisco 3600 series, and Cisco 3700 series routers.

Usage Guidelines

Use the **storm-control** command to block the forwarding of unnecessary flooded traffic.

Examples

The following example shows how to limit the threshold of broadcast traffic to 70 percent.

```
Router(config-if)# storm-control multicast 70
```

Related Commands

Command	Description
show interface counters	Displays the count of discarded packets.
show storm-control	Displays switchport characteristics, including storm-control levels set on the interface.

switchport mode

To set the interface type, use the **switchport mode** command in interface configuration mode. To reset the mode to the appropriate default mode for the device, use the appropriate **no** form of this command.

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

```
switchport mode {access | trunk}
```

Catalyst Switches

```
switchport mode {access | trunk | dynamic {auto | desirable}}
```

```
no switchport mode
```

```
switchport mode private-vlan {host | promiscuous}
```

```
no switchport mode private-vlan
```

Syntax Description

access	Specifies a nontrunking, nontagged single VLAN Layer 2 interface.
trunk	Specifies a trunking VLAN Layer 2 interface.
dynamic auto	Specifies that the interface convert the link to a trunk link.
dynamic desirable	Specifies that the interface actively attempt to convert the link to a trunk link.
private-vlan host	Specifies that the ports with a valid PVLAN association become active host private VLAN ports.
private-vlan promiscuous	Specifies that the ports with a valid PVLAN mapping become active promiscuous ports.

Defaults

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

The default is **access** mode.

Catalyst Switches

The default mode is dependent on the platform; it should be either **dynamic auto** for platforms that are intended as wiring closets or **dynamic desirable** for platforms that are intended as backbone switches. The default for PVLAN ports is that no mode is set.

Command Modes

Interface configuration

Command History

Release	Modification
12.0(7)XE	This command was introduced on the Catalyst 6000 family switches.
12.1(1)E	This command was integrated on the Catalyst 6000 family switches
12.1(8a)EX	The switchport mode private-vlan {host promiscuous} syntax was added.

Release	Modification
12.2(2)XT	Creation of switchports became available on Cisco 2600 series, Cisco 3600 series, and Cisco 3700 series routers.
12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T for creation of switchports on Cisco 2600 series, Cisco 3600 series, and Cisco 3700 series routers.

Usage Guidelines

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

If you enter a forced mode, the interface does not negotiate the link to the neighboring interface. Ensure that the interface ends match.

The **no** form of the command is not supported on the Cisco 2600 Series, Cisco 3600 Series, and Cisco 3700 Series Routers.

Catalyst Switches

If you enter **access** mode, the interface goes into permanent nontrunking mode and negotiates to convert the link into a nontrunk link even if the neighboring interface does not agree to the change.

If you enter **trunk** mode, the interface goes into permanent trunking mode and negotiates to convert the link into a trunk link even if the neighboring interface does not agree to the change.

If you enter **dynamic auto** mode, the interface converts the link to a trunk link if the neighboring interface is set to **trunk** mode or **desirable** mode.

If you enter **dynamic desirable** mode, the interface becomes a trunk interface if the neighboring interface is set to **trunk** mode, **desirable** mode, or **auto** mode.

If you configure a port as a promiscuous or host PVLAN port and one of the following applies, the port becomes inactive:

- The port does not have a valid PVLAN association or mapping configured.
- The port is a span destination.

Similarly, if a private port PVLAN association or mapping is deleted or if a private port is configured as a span destination, it becomes inactive.

Examples

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

The following example shows how to set the interface to **access** desirable mode:

```
Router(config-if)# switchport mode access
```

The following example shows how to set the interface to **trunk** mode:

```
Router(config-if)# switchport mode trunk
```

Catalyst Switches

The following example shows how to set the interface to dynamic desirable mode:

```
Router(config-if)# switchport mode dynamic desirable
```

The following example shows how to set a port to PVLAN **host** mode:

```
Router(config-if)# switchport mode private-vlan host
```

The following example shows how to set a port to PVLAN **promiscuous** mode:

```
Router(config-if)# switchport mode private-vlan promiscuous
```

Related Commands	Command	Description
	show interfaces switchport	Displays administrative and operational status of a switching (nonrouting) port.
	show interfaces trunk	
	switchport	Modifies the switching characteristics of the Layer 2-switched interface.
	switchport private-vlan host-association	Defines a PVLAN association for an isolated or community port.
	switchport private-vlan mapping	Defines the PVLAN mapping for a promiscuous port.

switchport trunk

To set the trunk characteristics when the interface is in trunking mode, use the **switchport trunk** commands in interface configuration mode. To reset all of the trunking characteristics back to the original defaults, use the **no** form of this command.

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

```
switchport trunk {encapsulation dot1q | native vlan | allowed vlan }
```

```
no switchport trunk {encapsulation dot1q | native vlan | allowed vlan }
```

Catalyst Switches

```
no switchport trunk {encapsulation isl | dot1q | negotiate } | { native vlan | allowed vlan | pruning vlan }
```

```
no switchport trunk {encapsulation {isl | dot1q | negotiate }} | { native vlan | allowed vlan | pruning vlan }
```

Syntax Description

allowed vlan <i>vlan-list</i>	Sets the list of allowed VLANs that transmit traffic from this interface in tagged format when in trunking mode. See the “Usage Guidelines” section for <i>vlan-list</i> formatting guidelines.
encapsulation dot1q	Sets the trunk encapsulation format to 802.1Q.
encapsulation isl	Sets the trunk encapsulation format to Inter-Switch Link (ISL).
encapsulation negotiate	Specifies that if the Dynamic Inter-Switch Link (DISL) protocol and Dynamic Packet Transport (DPT) negotiation do not resolve the encapsulation format, ISL is the selected format.
native vlan <i>vlan-id</i>	Sets the native VLAN for the trunk in 802.1Q trunking mode.
pruning vlan <i>vlan-list</i>	Sets the list of VLANs that are enabled for VTP pruning when in trunking mode. See the “Usage Guidelines” section for the <i>vlan-list</i> argument formatting guidelines.

Defaults

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

The default encapsulation type is dot1q.

The default access VLAN and trunk interface native VLAN is a default VLAN that corresponds to the platform or interface hardware.

The default for all VLAN lists is to include all VLANs.

Catalyst Switches

The default encapsulation type is dependent on the platform or interface hardware itself.

The default access VLAN and trunk interface native VLAN is a default VLAN corresponding to the platform or interface hardware.

The default for all VLAN lists is to include all VLANs.

Command Modes Interface configuration

Command History	Release	Modification
	12.0(7)XE	This command was introduced on the Catalyst 6000 family switch.
	12.1(1)E	switchport creation on Catalyst 6000 family switches was added.
	12.2(2)XT	This command was introduced to support switchport creation on Cisco 2600 series, Cisco 3600 series, and Cisco 3700 series routers.
	12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T to support switchport creation on Cisco 2600 series, Cisco 3600 series, and Cisco 3700 series routers.

Usage Guidelines

802.1Q trunks:

- When you connect Cisco switches through an 802.1Q trunk, make sure that the native VLAN for an 802.1Q trunk is the same on both ends of the trunk link. If the native VLAN on one end of the trunk is different from the native VLAN on the other end, spanning-tree loops might result.
- Disabling spanning tree on the native VLAN of an 802.1Q trunk without disabling spanning tree on every VLAN in the network can cause spanning-tree loops. Cisco recommends that you leave spanning tree enabled on the native VLAN of an 802.1Q trunk. If this is not possible, disable spanning tree on every VLAN in the network. Make sure that your network is free of physical loops before disabling spanning tree.
- When you connect two Cisco switches through 802.1Q trunks, the switches exchange spanning-tree BPDUs on each VLAN allowed on the trunks. The BPDUs on the native VLAN of the trunk are sent untagged to the reserved IEEE 802.1d spanning-tree multicast MAC address (01-80-C2-00-00-00). The BPDUs on all other VLANs on the trunk are sent tagged to the reserved Shared Spanning Tree Protocol (SSTP) multicast MAC address (01-00-0c-cc-cc-cd).
- The 802.1Q switches that are not Cisco switches maintain only a single instance of spanning-tree (the Mono Spanning Tree, or MST) that defines the spanning-tree topology for all VLANs. When you connect a Cisco switch to a switch through an 802.1Q trunk without a Cisco switch, the MST of the switch and the native VLAN spanning tree of the Cisco switch combine to form a single spanning-tree topology known as the CST.
- Because Cisco switches transmit BPDUs to the SSTP multicast MAC address on VLANs other than the native VLAN of the trunk, switches that are not Cisco switches do not recognize these frames as BPDUs and flood them on all ports in the corresponding VLAN. Other Cisco switches connected to the 802.1Q cloud receive these flooded BPDUs. This allows Cisco switches to maintain a per-VLAN spanning-tree topology across a cloud of 802.1Q switches that are not Cisco switches. The 802.1Q cloud of switches separating the Cisco switches is treated as a single broadcast segment among all switches connected to the 802.1Q cloud of switches that are not Cisco switches through 802.1Q trunks.
- Make certain that the native VLAN is the same on *all* of the 802.1Q trunks that connects the Cisco switches to the 802.1Q cloud of switches that are not Cisco switches.
- If you are connecting multiple Cisco switches to a non-Cisco 802.1Q cloud, all of the connections must be through 802.1Q trunks. You cannot connect Cisco switches to a non-Cisco 802.1Q cloud through ISL trunks or through access ports. Doing so will cause the switch to place the ISL trunk port or access port into the spanning-tree “port inconsistent” state and no traffic will pass through the port.

no switchport trunk native vlan Form of the Command

The **no** form of the **no switchport trunk native vlan** command resets the native mode VLAN to the appropriate default VLAN for the device.

no switchport trunk allowed vlan Form of the Command

The **no** form of the **no switchport trunk allowed vlan** command resets the list to the default list, which allows all VLANs.

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

The **switchport trunk encapsulation** command is supported only for platforms and interface hardware that can support 802.1Q formats.

The *vlan-list* format is **all | none | add | remove | except** *vlan-list[,vlan-list...]* where:

- **all**—Specifies all VLANs from 1 to 1005.
- **none**—Indicates an empty list. This keyword is not supported in the **switchport trunk allowed vlan** form of the command.
- **add**—Adds the defined list of VLANs to those currently set instead of replacing the list.
- **remove**—Removes the defined list of VLANs from those currently set instead of replacing the list.
- **except**—Lists the VLANs that should be calculated by inverting the defined list of VLANs.
- *vlan-list*—is either a single VLAN number from 1 to 1005 or a continuous range of VLANs described by two VLAN numbers, the lesser one first, separated by a hyphen that represents the VLAN IDs of the allowed VLANs when this port is in trunking mode.

Catalyst Switches

The **switchport trunk encapsulation** command is supported only for platforms and interface hardware that can support both ISL and 802.1Q formats.

If you enter the **negotiate** keyword and DISL and DTP negotiation do not resolve the encapsulation format, ISL is the selected format. The **no** form of the command resets the trunk encapsulation format back to the default.

The **no** form of the **switchport trunk {encapsulation {isl | dot1q | negotiate} pruning vlan** command resets the list to the default list, which enables all VLANs for VTP pruning.

The *vlan-list* format is **all | none | add | remove | except** *vlan-list[,vlan-list...]* where:

- **all**—Specifies all VLANs from 1 to 1005. This keyword is not supported in the **switchport trunk pruning vlan** command.
- **none**—Indicates an empty list. This keyword is not supported in the **switchport trunk allowed vlan** command.
- **add**—Adds the defined list of VLANs to those currently set, instead of replacing the list.
- **remove**—Removes the defined list of VLANs from those currently set instead of replacing the list.
- **except**—Lists the VLANs that should be calculated by inverting the defined list of VLANs.
- *vlan-list*—Is either a single VLAN number from 1 to 1005 or a continuous range of VLANs described by two VLAN numbers, the lesser one first, separated by a hyphen that represents the VLAN IDs of the allowed VLANs when this port is in trunking mode.

Examples

The following example shows how to cause a port interface configured as a switched interface to encapsulate in 802.1Q trunking format regardless of its default trunking format in trunking mode:

```
Router(config-if)# switchport trunk encapsulation dot1q
```

Related Commands

Command	Description
show interfaces switchport	Displays administrative and operational status of a switching (nonrouting) port.

switchport voice vlan

To configure the voice VLAN on the port, use the **switchport voice vlan** command in interface configuration mode. To return the setting to its default, use the **no** form of this command.

```
switchport voice vlan {vlan-id | dot1p | none | untagged}
```

```
no switchport voice vlan
```

Syntax Description		
<i>vlan-id</i>	VLAN used for voice traffic. Valid IDs are from 1 to 1005 (IDs 1006 to 4096 are not supported).	Do not enter leading zeros. The switch port is an 802.1Q trunk port.
dot1p	The telephone uses priority tagging and uses VLAN 0. The switch port is an 802.1Q trunk port.	
none	The telephone is not instructed through the command-line interface (CLI) about the voice VLAN. The telephone uses the configuration from the telephone keypad.	
untagged	The telephone does not tag frames; it uses VLAN 4095. The switch port can be an access port or an 802.1Q trunk port.	

Defaults

The switch default is to not automatically configure the telephone (**none**).

The Cisco IP 7960 telephone default is to generate an 802.1Q/802.1P frame.

Command Modes

Interface configuration

Command History

Release	Modification
12.2(2)XT	This command was introduced.
12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T to support creation of switchports.

Usage Guidelines

Ports that are not configured as trunk ports but that have a configured voice VLAN are access ports with a voice VLAN ID (VVID).

Examples

The following example shows how to configure VLAN 2 as the voice VLAN:

```
Switch(config-if)# switchport voice vlan 2
```

test aim eeprom

To test the data compression Advanced Interface Module (AIM) after it is installed in the Cisco 2600 router, use the **test aim eeprom** command in global configuration mode.

test aim eeprom

Syntax Description This command has no arguments or keywords.

Defaults Disabled

Command Modes Global configuration

Command History	Release	Modification
	12.0(2)T	This command was introduced.

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



Caution

Using this command can erase all locations in EEPROM memory.

This command is the AIM counterpart of the **test pas eeprom** command, which performs similar tasks for port modules.

[Table 52](#) shows the questions asked of the user when the **test aim eeprom** command is entered, and the recommended user responses.

Table 52 test aim eeprom Command Questions and Responses

Questions	Responses
AIM Slot [0]:	User responds by entering the slot number of the AIM whose EEPROM is to be modified. If the user presses ENTER, the default slot 0 is used.
Use NMC93C46 ID EEPROM [y]:	User responds with “y” if the AIM contains an NMC93C46 type EEPROM and “n” if the AIM contains an X2444 EEPROM. The compression Advanced Interface Module (CAIM) contains a NMC93C46 EEPROM, and this is the default if the user just pressed ENTER.
AIM Slot %d eeprom (? for help)[%c]	General command prompt for the test aim eeprom command dialog. The AIM slot number chosen is displayed, and the default command is the last command entered.

Table 52 test aim eeprom Command Questions and Responses (continued)

Questions	Responses
Address within slot %d eeprom, [0x%02x]	Enter the desired address within the EEPROM to modify. The default is the next address beyond the byte last modified. If the user wishes to enter a hexadecimal number, it must be preceded by "0x".
Read or Write access to slot %d at 0x%02x [%c]?	Respond with a W to write to the addressed byte or with an R to read from the addressed byte. The default value is selected by just pressing Enter and is the same as the value specified in the last primitive access.
Write data (hex 8 bits) [%02x]?:	If you respond to prompt B with "W", then prompt C is issued, requesting the user to enter the data to write to the addressed byte. The user enters the desired value. Note that if the user desires to enter a hex value, the hex value entered must be preceded by "0x". Otherwise, the value entered is assumed to be in decimal radix.

There is a danger that you can erase all bytes in the entire EEPROM. Though it is good to have a diagnostic tool that allows you to read and write data, there is a danger that lost data will make the Advanced Interface Module (AIM) card fail.

During your session with the test dialog, you have access to the following commands:

H or h	Displays a summary of the available commands.
d	Dump EEPROM contents—Displays the contents of the EEPROM in hex.
e	Erase EEPROM—Erases the entire EEPROM (all bytes set to 0xff).
p	Primitive access—Erases the EEPROM.
q	Exit EEPROM test—Causes the test aim eeprom command dialog to exit to the command line interface (CLI).
z	Zero EEPROM—Zeros the entire EEPROM.

Examples

The following example displays the **test aim eeprom** command user dialog:

```
Router# test aim eeprom
AIM Slot [0]: 0
Use NMC93C46 ID EEPROM [y]: y
AIM Slot 0 eeprom (? for help)[?]: ?
  d - dump eeprom contents
  e - erase all locations (to 1)
  p - primitive access
  q - exit eeprom test
  z - zero eeprom

'c' rules of radix type-in and display apply.

AIM Slot 0 eeprom (? for help)[?]:
```

test interface fastethernet

To test the Fast Ethernet interface by causing the interface to ping itself, use the **test interface fastethernet** command in user EXEC and privileged EXEC mode.

test interface fastethernet *number*

Syntax Description	<i>number</i>	Port, connector, or interface card number. On a Cisco 4500 or Cisco 4700 series router, specifies the network processor module (NPM) number. The numbers are assigned at the factory at the time of installation or when added to a system and are displayed with the show interfaces command.
---------------------------	---------------	---

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

Command History	Release	Modification
	11.2	This command was introduced.

Usage Guidelines	This command sends pings from the specified interface to itself. Unlike the ping command, the test interface fastethernet command does not require the use of an IP address. This command does not have a no form.
-------------------------	--

Examples	The following example tests a Fast Ethernet interface on a Cisco 4500 router: Router# test interface fastethernet 0
-----------------	---

Related Commands	Command	Description
	ping (privileged)	Diagnoses basic network connectivity on AppleTalk, CLNS, DECnet, IP, or Novell IPX networks.
	ping (user)	Provides simple ping diagnostics of network connectivity.

test service-module

To perform self-tests on an integrated CSU/DSU serial interface module, such as a 4-wire, 56/64 kbps CSU/DSU, use the **test service-module** command in privileged EXEC command.

test service-module *type number*

Syntax Description

<i>type</i>	Interface type.
<i>number</i>	Interface number.

Command Modes

Privileged EXEC

Command History

Release	Modification
11.2	This command was introduced.

Usage Guidelines

The following tests are performed on the CSU/DSU:

- ROM checksum test
- RAM test
- EEPROM checksum test
- Flash checksum test
- DTE loopback with an internal pattern test

These self-tests are also performed at power on.

This command cannot be used if a DTE loopback, line loopback, or remote loopback is in progress.

Data transmission is interrupted for 5 seconds when you issue this command. To view the output of the most recent self-tests, use the **show service-module** command.

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

Examples

This example performs a self-test on serial interface 0:

```
Router# test service-module serial 0
SERVICE_MODULE(0): Performing service-module self test
SERVICE_MODULE(0): self test finished: Passed
```

Related Commands

Command	Description
channelized	Clears the interface counters.
clear service-module serial	Resets an integrated CSU/DSU.
show service-module serial	Displays the performance report for an integrated CSU/DSU.

timeslot

To enable framed mode on a serial interface on a G.703 E1 port adapter, an FSIP, or an E1-G.703/G.704 serial port adapter, use the **timeslot** command in interface configuration mode. To restore the interface to unframed mode, use the **no** form of this command or set the start slot to 0.

timeslot *start-slot stop-slot*

no timeslot

Syntax Description

<i>start-slot</i>	First subframe in the major frame. Valid range is 1 to 31 and must be less than or equal to <i>stop-slot</i> .
<i>stop-slot</i>	Last subframe in the major frame. Valid range is 1 to 31 and must be greater than or equal to <i>start-slot</i> .

Defaults

The default G.703 E1 interface is not configured for framed mode.

Command Modes

Interface configuration

Command History

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

Usage Guidelines

Framed mode allows you to specify a bandwidth for the interface by designating some of the 32 time slots for data and reserving the others for framing (timing). Unframed mode, also known as clear channel, does not reserve any time slots for framing.

This command applies to Cisco 4000, 7000, 7200, and 7500 series routers. G.703 E1 interfaces have two modes of operation, framed and unframed. When in framed mode, the range from *start-slot* to *stop-slot* gives the number of 64-kbps slots in use. There are 32 64-kbps slots available.

In framed mode, timeslot 16 is not used for data. To use timeslot 16 for data, use the **ts16** interface configuration command.

Examples

The following example enables framed mode on a serial interface on a G.703 E1 port adapter or a E1-G.703/G.704 port adapter:

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

Related Commands

Command	Description
ts16	Controls the use of timeslot 16 for data on a G.703 E1 interface or on an E1-G703/G.704 serial port adapter.

transmit-buffers backing-store

To buffer short-term traffic bursts that exceed the bandwidth of the output interface, use the **transmit-buffers backing-store** command in interface configuration mode. To disable this function, use the **no** form of this command.

transmit-buffers backing-store

no transmit-buffers backing-store

Syntax Description This command has no arguments or keywords.

Defaults The default is off, unless weighted fair queuing is enabled on the interface. If weighted fair queuing is enabled on the interface, the **transmit-buffers backing-store** command is enabled by default.

Command Modes Interface configuration

Command History	Release	Modification
	10.3	This command was introduced on the Cisco 7500 series router.

Usage Guidelines If the **transmit-buffers backing-store** command is enabled and a full hardware transmit queue is encountered, packets are swapped out of the original memory device (MEMD) into a system buffer in DRAM. If the **transmit-buffers backing-store** command is *not* enabled and the output hold queue is full, packets are dropped instead of being copied if a full hardware transmit queue is encountered. In both cases, the original MEMD buffer is freed so that it can be reused for other input packets.

To preserve packet order, the router checks the output hold queue and outputs previously queued packets first.

Examples The following example shows how to enable the **transmit-buffers backing-store** command on a FDDI interface:

```
Router(config)# interface fddi 3/0
Router(config-if)# transmit-buffers backing-store
```

Related Commands	Command	Description
	fair-queue (WFQ)	Enables WFQ for an interface.

transmit-clock-internal

To enable the internally generated clock on a serial interface on a Cisco 7200 series or Cisco 7500 series router when a DTE does not return a transmit clock, use the **transmit-clock-internal** command in interface configuration mode. To disable the feature, use the **no** form of this command.

transmit-clock-internal

no transmit-clock-internal

Syntax Description This command has no arguments or keywords.

Defaults Disabled

Command Modes Interface configuration

Release	Modification
10.0	This command was introduced.

Examples The following example enables the internally generated clock on serial interface 3/0 on a Cisco 7000 series or Cisco 7500 series router:

```
Router(config)# interface serial 3/0  
Router(config-if)# transmit-clock-internal
```

transmitter-delay

To specify a minimum dead-time after transmitting a packet, use the **transmitter-delay** command in interface configuration mode. To restore the default, use the **no** form of this command.

transmitter-delay *delay*

no transmitter-delay

Syntax Description	<i>delay</i>	On the FSIP, high-speed serial interface (HSSI, and) on the IGS router, the minimum number of High-Level Data Link Control (HDLC) flags to be sent between successive packets. On all other serial interfaces and routers, approximate number of microseconds of minimum delay after transmitting a packet. The valid range is 0 to 13,1071. The default is 0.
Defaults	0 flags or microseconds	
Command Modes	Interface configuration	
Command History	Release	Modification
	10.0	This command was introduced.
Usage Guidelines	<p>This command is especially useful for serial interfaces that can send back-to-back data packets over serial interfaces faster than some hosts can receive them.</p> <p>The transmitter delay feature is implemented for the following Token Ring cards: CSC-R16, CSC-R16M, CSC-1R, CSC-2R, and CSC-CTR. For the first four cards, the command syntax is the same as the existing command and specifies the number of microseconds to delay between sending frames that are generated by the router. Transmitter delay for the CSC-CTR uses the same syntax, but specifies a relative time interval to delay between transmission of all frames.</p>	
Examples	<p>The following example specifies a delay of 300 microseconds on serial interface 0:</p> <pre>Router(config)# interface serial 0 Router(config-if)# transmitter-delay 300</pre>	

ts16

To control the use of time slot 16 for data on a G.703 E1 interface or on a E1-G.703/G.704 serial port adapter, use the **ts16** command in interface configuration mode. To restore the default, use the **no** form of this command.

ts16

no ts16

Syntax Description

This command has no arguments or keywords.

Defaults

Time slot 16 is used for signaling.

Command Modes

Interface configuration

Command History

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

Usage Guidelines

This command applies to Cisco 4000, 7000, 7200, and 7500 series routers. By default, time slot 16 is used for signaling. Use this command to configure time slot 16 to be used for data. When in framed mode, in order to get all possible subframes or time slots, you must use the **ts16** command.

Examples

The following example configures time slot 16 to be used for data on a G.703 E1 interface or a E1-G.703/G.704 serial port adapter:

```
Router(config-if)# ts16
```

Related Commands

Command	Description
timeslot	Enables framed mode serial interface on a G.703 E1 port adapter, an FSIP, or an E1-G.703/G.704 serial port adapter.

tunnel checksum

To enable encapsulator-to-decapsulator checksumming of packets on a tunnel interface, use the **tunnel checksum** command in interface configuration mode. To disable checksumming, use the **no** form of this command.

tunnel checksum

no tunnel checksum

Syntax Description This command has no arguments or keywords.

Defaults Disabled

Command Modes Interface configuration

Command History	Release	Modification
	10.0	This command was introduced.

Usage Guidelines This command currently applies to generic route encapsulation (GRE) only. Some passenger protocols rely on media checksums to provide data integrity. By default, the tunnel does not guarantee packet integrity. By enabling end-to-end checksums, the routers will drop corrupted packets.

Examples In the following example, all protocols will have encapsulator-to-decapsulator checksumming of packets on the tunnel interface:

```
Router(config-if)# tunnel checksum
```

tunnel destination

To specify the destination for a tunnel interface, use the **tunnel destination** command in interface configuration mode. To remove the destination, use the **no** form of this command.

tunnel destination {*hostname* | *ip-address*}

no tunnel destination

Syntax Description

<i>hostname</i>	Name of the host destination.
<i>ip-address</i>	IP address of the host destination expressed in decimal in four-part, dotted notation.

Defaults

No tunnel interface destination is specified.

Command Modes

Interface configuration

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines

You cannot have two tunnels using the same encapsulation mode with exactly the same source and destination address. The workaround is to create a loopback interface and source packets off of the loopback interface. Refer to *Cisco IOS AppleTalk and Novell IPX Configuration Guide* for more information on AppleTalk Cayman tunneling.

Examples

The following example enables Cayman tunneling:

```
Router(config)# interface tunnel0
Router(config-if)# tunnel source ethernet0
Router(config-if)# tunnel destination 10.108.164.19
Router(config-if)# tunnel mode cayman
```

The following example enables GRE (generic routing encapsulation) tunneling:

```
Router(config)# interface tunnel0
Router(config-if)# appletalk cable-range 4160-4160 4160.19
Router(config-if)# appletalk zone Engineering
Router(config-if)# tunnel source ethernet0
Router(config-if)# tunnel destination 10.108.164.19
Router(config-if)# tunnel mode gre ip
```

Related Commands	Command	Description
	appletalk cable-range	Enables an extended AppleTalk network.
	appletalk zone	Sets the zone name for the connected AppleTalk network.
	tunnel mode	Sets the encapsulation mode for the tunnel interface.
	tunnel source	Sets the source address of a tunnel interface.

tunnel key

To enable an ID key for a tunnel interface, use the **tunnel key** command in interface configuration mode. To remove the ID key, use the **no** form of this command.

tunnel key *key-number*

no tunnel key

Syntax Description	<i>key-number</i>	Number from 0 to 4,294,967,295 that identifies the tunnel key.
--------------------	-------------------	--

Defaults	Disabled
----------	----------

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

Command History	Release	Modification
	10.0	This command was introduced.

Usage Guidelines This command currently applies to generic route encapsulation (GRE) only. Tunnel ID keys can be used as a form of *weak* security to prevent improper configuration or injection of packets from a foreign source.



Note

IP multicast traffic is not supported when a tunnel ID key is configured unless the traffic is process-switched. You must configure the **no ip mroute-cache** command in interface configuration mode on the interface if an ID key is configured. This note applies only to Cisco IOS Release 12.0 and earlier releases.



Note

When GRE is used, the ID key is carried in each packet. We do *not* recommend relying on this key for security purposes.

Examples The following example sets the tunnel key to 3:

```
Router(config-if)# tunnel key 3
```

tunnel mode

To set the encapsulation mode for the tunnel interface, use the **tunnel mode** command in interface configuration mode. To restore the default mode, use the **no** form of this command.

```
tunnel mode { aurp | cayman | dvmrp | eon | gre | gre multipoint | ipip [decapsulate-any] | iptalk
  | mpls | nos }
```

```
no tunnel mode
```

Syntax Description	
aurp	AppleTalk Update-Based Routing Protocol.
cayman	Cayman TunnelTalk AppleTalk encapsulation.
dvmrp	Distance Vector Multicast Routing Protocol.
eon	EON compatible CLNS tunnel.
gre	Generic routing encapsulation protocol. This is the default.
gre multipoint	Multipoint GRE (mGRE).
ipip	IP-over-IP encapsulation.
decapsulate-any	(Optional) Terminates any number of IP-in-IP tunnels at one tunnel interface. Note that this tunnel will not carry any outbound traffic; however, any number of remote tunnel endpoints can use a tunnel configured this way as their destination.
iptalk	Apple IPTalk encapsulation.
mpls	Multiprotocol Label Switching encapsulation.
nos	KA9Q/NOS compatible IP over IP.

Defaults GRE tunneling

Command Modes Interface configuration

Command History	Release	Modification
	10.0	This command was introduced.
	10.3	The following keywords were added: <ul style="list-style-type: none"> • aurp • dvmrp • ipip
	11.2	The optional decapsulate-any keyword was added.
	12.2(13)T	The gre multipoint keyword was added.

Usage Guidelines**Source and Destination Address**

You cannot have two tunnels that use the same encapsulation mode with exactly the same source and destination address. The workaround is to create a loopback interface and source packets off of the loopback interface.

Cayman Tunneling

Designed by Cayman Systems, Cayman tunneling implements tunneling to enable Cisco routers to interoperate with Cayman GatorBoxes. With Cayman tunneling, you can establish tunnels between two routers or between a Cisco router and a GatorBox. When using Cayman tunneling, you must not configure the tunnel with an AppleTalk network address.

DVMRP

Use DVMRP when a router connects to an mrouter to run DVMRP over a tunnel. You must configure Protocol Independent Multicast (PIM) and an IP address on a DVMRP tunnel.

GRE with AppleTalk

GRE tunneling can be done between Cisco routers only. When using GRE tunneling for AppleTalk, you configure the tunnel with an AppleTalk network address. Using the AppleTalk network address you can ping the other end of the tunnel to check the connection.

Multipoint GRE

After enabling mGRE tunneling, you can enable the **tunnel protection** command, which allows you to associate the mGRE tunnel with an IP Security (IPSec) profile. Combining mGRE tunnels and IPSec encryption allows a single mGRE interface to support multiple IPSec tunnels, thereby simplifying the size and complexity of the configuration.

**Note**

GRE tunnel keepalives configured using the **keepalive** command under GRE interface are supported only on point-to-point GRE tunnels.

Examples**Cayman Tunneling**

The following example enables Cayman tunneling:

```
Router(config)# interface tunnel 0
Router(config-if)# tunnel source ethernet 0
Router(config-if)# tunnel destination 10.108.164.19
Router(config-if)# tunnel mode cayman
```

GRE Tunneling

The following example enables GRE tunneling:

```
Router(config)# interface tunnel 0
Router(config-if)# appletalk cable-range 4160-4160 4160.19
Router(config-if)# appletalk zone Engineering
Router(config-if)# tunnel source ethernet0
Router(config-if)# tunnel destination 10.108.164.19
Router(config-if)# tunnel mode gre
```

Multipoint GRE Tunneling

The following example shows how to enable mGRE tunneling:

```
interface Tunnel0
```

```

bandwidth 1000
ip address 10.0.0.1 255.255.255.0
! Ensures longer packets are fragmented before they are encrypted; otherwise, the
! receiving router would have to do the reassembly.
ip mtu 1416
! Turns off split horizon on the mGRE tunnel interface; otherwise, EIGRP will not
! advertise routes that are learned via the mGRE interface back out that interface.
no ip split-horizon eigrp 1
no ip next-hop-self eigrp 1
delay 1000
! Sets IPsec peer address to Ethernet interface's public address.
tunnel source Ethernet0
tunnel mode gre multipoint
! The following line must match on all nodes that want to use this mGRE tunnel.
tunnel key 100000
tunnel protection ipsec profile vpnprof

```

Related Commands

Command	Description
appletalk cable-range	Enables an extended AppleTalk network.
appletalk zone	Sets the zone name for the connected AppleTalk network.
tunnel destination	Specifies the destination for a tunnel interface.
tunnel protection	Associates a tunnel interface with an IPsec profile.
tunnel source	Sets the source address of a tunnel interface.

tunnel path-mtu-discovery

To enable Path MTU Discovery (PMTUD) on a GRE or IP-in-IP tunnel interface, use the **tunnel path-mtu-discovery** command in interface configuration mode. To disable PMTUD on a tunnel interface, use the **no** form of this command.

```
tunnel path-mtu-discovery [age-timer {aging-mins | infinite}]
```

```
no tunnel path-mtu-discovery
```

Syntax Description

age-timer	(Optional) Sets a timer to run for a specified interval, in minutes, after which the tunnel interface resets the maximum transmission unit (MTU) of the path to the default tunnel MTU minus 24 bytes for GRE tunnels or minus 20 bytes for IP-in-IP tunnels. <ul style="list-style-type: none"> <i>aging-mins</i>—Number of minutes. Range is from 10 to 30. Default is 10. infinite—Disables the age timer.
------------------	--

Defaults

Path MTU Discovery is disabled for a tunnel interface.

Command Modes

Interface configuration

Command History

Release	Modification
12.0(5)WC5	This command was introduced.
12.0(7)T3	This command was integrated into Cisco IOS Release 12.0(7)T3.

Usage Guidelines

When PMTUD (RFC 1191) is enabled on a tunnel interface, the router performs PMTUD processing for the GRE (or IP-in-IP) tunnel IP packets. The router always performs PMTUD processing on the original data IP packets that enter the tunnel. When PMTUD is enabled, no packet fragmentation occurs on the encapsulated packets that travel through the tunnel. Without packet fragmentation, there is a better throughput of TCP connections, and this makes PMTUD a method for maximizing the use of available bandwidth in the network between the endpoints of a tunnel interface.

After PMTUD is enabled, the Don't Fragment (DF) bit of the IP packet header that is forwarded into the tunnel is copied to the IP header of the external IP packets. The external IP packet is the encapsulating IP packet. Adding the DF bit allows the PMTUD mechanism to work on the tunnel path of the tunnel. The tunnel endpoint listens for ICMP unreachable too-big messages and modifies the IP MTU of the tunnel interface, if required.

When the aging timer is configured, the tunnel code resets the tunnel MTU after the aging timer expires. After the tunnel MTU is reset, a set of full-size packets with the DF bit set is required to trigger the tunnel PMTUD and lower the tunnel MTU. At least two packets are dropped each time the tunnel MTU changes.

When PMTUD is disabled, the DF bit of an external (encapsulated) IP packet is set to zero even if the encapsulated packet has a DF bit set to one.

**Note**

PMTUD on a tunnel interface requires that the tunnel endpoint be able to receive ICMP messages generated by routers in the path of the tunnel. Check that ICMP messages can be received before using PMTUD over firewall connections.

PMTUD currently works only on GRE and IP-in-IP tunnel interfaces.

Use the **show interfaces tunnel** command to verify the tunnel PMTUD parameters.

Examples

The following example shows how to enable tunnel PMTUD:

```
Router(config)# interface tunnel 0  
Router(config-if)# tunnel path-mtu-discovery
```

Related Commands

Command	Description
interface	Configures an interface and enters interface configuration mode.
show interfaces tunnel	Displays information about the specified tunnel interface.

tunnel sequence-datagrams

To configure a tunnel interface to drop datagrams that arrive out of order, use the **tunnel sequence-datagrams** command in interface configuration mode. To disable this function, use the **no** form of this command.

tunnel sequence-datagrams

no tunnel sequence-datagrams

Syntax Description This command has no arguments or keywords.

Defaults Disabled

Command Modes Interface configuration

Release	Modification
10.0	This command was introduced.

Usage Guidelines This command currently applies to generic route encapsulation (GRE) only. This command is useful when carrying passenger protocols that behave poorly when they receive packets out of order (for example, LLC2-based protocols).

Examples The following example configures the tunnel to drop datagrams that arrive out of order:

```
Router(config-if)# tunnel sequence-datagrams
```

tunnel source

To set source address for a tunnel interface, use the **tunnel source** command in interface configuration mode. To remove the source address, use the **no** form of this command.

tunnel source {*ip-address* | *type number*}

no tunnel source

Syntax Description		
	<i>ip-address</i>	IP address to use as the source address for packets in the tunnel.
	<i>type</i>	Interface type.
	<i>number</i>	Specifies the port, connector, or interface card number. The numbers are assigned at the factory at the time of installation or when added to a system and can be displayed with the show interfaces command.

Defaults No tunnel interface source address is set.

Command Modes Interface configuration

Command History	Release	Modification
	10.0	This command was introduced.

Usage Guidelines You cannot have two tunnels using the same encapsulation mode with exactly the same source and destination address. The workaround is to create a loopback interface and source packets off of the loopback interface.

When using tunnels to Cayman boxes, you must set the **tunnel source** command to an explicit IP address on the same subnet as the Cayman box, not the tunnel itself.

Examples The following example enables Cayman tunneling:

```
Router(config)# interface tunnel0
Router(config-if)# tunnel source ethernet0
Router(config-if)# tunnel destination 131.108.164.19
Router(config-if)# tunnel mode cayman
```

The following example enables GRE (generic routing encapsulation) tunneling:

```
Router(config)# interface tunnel0
Router(config-if)# appletalk cable-range 4160-4160 4160.19
Router(config-if)# appletalk zone Engineering
Router(config-if)# tunnel source ethernet0
Router(config-if)# tunnel destination 131.108.164.19
Router(config-if)# tunnel mode gre ip
```

Related Commands

Command	Description
appletalk cable-range	Enables an extended AppleTalk network.
appletalk zone	Sets the zone name for the connected AppleTalk network.
tunnel destination	Specifies the destination for a tunnel interface.

tx-queue-limit

To control the number of transmit buffers available to a specified interface on the MCI and SCI cards, use the **tx-queue-limit** command in interface configuration mode.

tx-queue-limit *number*

Syntax Description	<i>number</i>	Maximum number of transmit buffers that the specified interface can subscribe.
--------------------	---------------	--

Defaults	Defaults depend on the total transmit buffer pool size and the traffic patterns of all the interfaces on the card. Defaults and specified limits are displayed with the show controllers mci EXEC command.
----------	---

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

Command History	Release	Modification
	10.0	This command was introduced.

Usage Guidelines	This command should be used only under the guidance of a technical support representative. This command does not have a no form.
------------------	--

Examples	The following example sets the maximum number of transmit buffers on the interface to 5:
----------	--

```
Router(config)# interface ethernet 0
Router(config-if)# tx-queue-limit 5
```

Related Commands	Command	Description
	show controllers mci	Displays all information under the MCI card or the SCI.

yellow

To enable generation and detection of yellow alarms, use the **yellow** command in interface configuration mode.

```
yellow {generation | detection}
```

Syntax Description

<i>generation</i>	This setting enables or disables generation of yellow alarms.
<i>detection</i>	This setting enables or disables detection of yellow alarms.

Defaults

Yellow alarm generation and detection are enabled.

Command Modes

Interface Configuration

Command History

Release	Modification
12.0(5)XE	This command was introduced.
12.0(7)XE1	Support for Cisco 7100 series routers added.
12.1(5)T	This command was integrated into Cisco IOS Release 12.1(5)T.

Usage Guidelines

Use this command to generate and detect yellow alarms.

Examples

The following example enables generation and detection of yellow alarms on a Cisco 7500 series router:

```
Router(config)# interface atm 3/1/0
Router(config-if)# yellow generation
Router(config-if)# yellow detection
```

Related Commands

Command	Description
show controllers [<i>atm slot/ima group-number</i>]	Displays detailed information about IMA groups and the links they include, as well as about current queues.

