

# t1

To create a logical T1 controller from each of the specified time slots of the T3 line, use the **t1** command in controller configuration mode. To delete the defined logical controller, use the **no** form of this command.

**t1** *dsl* **controller**

**no t1** *dsl* **controller**

## Syntax Description

*dsl* Time slot within the T3 line. The valid time-slot range is from 1 to 28.

## Defaults

No default behavior or values.

## Command Modes

Controller configuration

## Command History

Release	Modification
11.3AA	This command was introduced.

## Usage Guidelines

The purpose of this command is to convert the collection of the 28 T1 controllers comprising the T3 controller into individual T1 controllers that the system can use. In other words, the Cisco AS5800 access server cannot pass data until a T1 controller is configured (using the **controller** command), and you cannot configure a T1 controller until it has been created using the **t1** command.

## Examples

The following example shows how to configure a logical T1 controller at T1 time slot 1 for the T3 controller located in shelf 1, slot 4, port 0. Note that you have to enter the command from controller configuration mode.

```
Router(config)# controller t3 1/4/0
Router(config-controller)# t1 1 controller
Router(config-controller)# end
```

## Related Commands

Command	Description
<b>controller</b>	Configures a T1 and other types of controller and enters controller configuration mode.
<b>controller t3</b>	Configures a T3 controller.

# t1 bert

To enable or disable a bit error rate tester (BERT) test pattern for a T1 channel on the Channelized T3 Interface Processor (CT3IP) in Cisco 7500 series routers, use the **t1 bert** command in controller configuration mode. To disable a BERT test pattern, use the **no** form of this command.

**t1 channel bert pattern** {0s | 1s | 2<sup>15</sup> | 2<sup>20</sup> | 2<sup>23</sup>} **interval** *minutes* [**unframed**]

**no t1 channel bert pattern** {0s | 1s | 2<sup>15</sup> | 2<sup>20</sup> | 2<sup>23</sup>} **interval** *minutes* [**unframed**]

## Syntax Description

<i>channel</i>	Number between 1 and 28 that indicates the T1 channel.
<b>pattern</b>	Specifies the length of the repeating BERT test pattern.
<b>0s</b>	0s—Repeating pattern of zeros (...000...).
<b>1s</b>	1s—Repeating pattern of ones (...111...).
<b>2<sup>15</sup></b>	2 <sup>15</sup> —Pseudorandom repeating pattern that is 32,767 bits in length.
<b>2<sup>20</sup></b>	2 <sup>20</sup> —Pseudorandom repeating pattern that is 1,048,575 bits in length.
<b>2<sup>23</sup></b>	2 <sup>23</sup> —Pseudorandom repeating pattern that is 8,388,607 bits in length.
<b>interval</b> <i>minutes</i>	Specifies the duration of the BERT test, in minutes. The interval can be a value from 1 to 14400.
<b>unframed</b>	(Optional) Specifies T1 unframed BERT.

## Defaults

No BERT test is performed.

## Command Modes

Controller configuration

## Command History

Release	Modification
11.3	This command was introduced.
12.2S	The <b>unframed</b> keyword was added to this command.

## Usage Guidelines

The BERT test patterns from the CT3IP are framed test patterns (that is, the test patterns are inserted into the payload of the framed T1 signal).

To view the BERT results, use the **show controller t3** or **show controller t3 brief EXEC** commands. The BERT results include the following information:

- Type of test pattern selected
- Status of the test
- Interval selected
- Time remaining on the BERT test
- Total bit errors
- Total bits received

When the T1 channel has a BERT test running, the line state is DOWN. Also, when the BERT test is running and the Status field is Not Sync, the information in the total bit errors field is not valid. When the BERT test is done, the Status field is not relevant.

The **t1 bert** command is not written to NVRAM because it is only used for testing the T1 channel for a short predefined interval and for avoiding accidentally saving the command, which could cause the interface not to come up the next time the router reboots.

**Note**

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.

**Examples**

The following example shows how to run a BERT test pattern of all zeros for 30 minutes on T1 channel 6 on the CT3IP in slot 9:

```
Router(config)# controller t3 9/0/0
Router(config-controller)# t1 6 bert pattern 0s interval 30
```

**Related Commands**

Command	Description
<b>show controllers t3</b>	Displays the hardware and software driver information for a T3 controller.

# t1 clock source

To specify where the clock source is obtained for use by each T1 channel on the Channelized T3 Interface Processor (CT3IP) in Cisco 7500 series routers, use the **t1 clock source** command in controller configuration mode.

```
t1 channel clock source {internal | line}
```

Syntax Description	channel	Number between 1 and 28 that indicates the T1 channel.
	<b>internal</b>	Specifies that the internal clock source is used. This is the default.
	<b>line</b>	Specifies that the network clock source is used.

**Defaults** Internal

**Command Modes** Controller configuration

Command History	Release	Modification
	11.3	This command was introduced.

**Usage Guidelines** If you do not specify the **t1 clock source** command, the default clock source of **internal** is used by all the T1s on the CT3IP.

You can also set the clock source for the CT3IP by using the **clock source** (CT3IP) controller configuration command.



**Note**

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.

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

**Examples** The following example shows how to set the clock source to line T1 6 and T1 8 on the CT3IP:

```
Router(config)# controller t3 9/0/0
Router(config-controller)# t1 6 clock source line
Router(config-controller)# t1 8 clock source line
```

Related Commands	Command	Description
	<b>clock source</b> (CT3IP)	Specifies where the clock source is obtained for use by the CT3IP in Cisco 7500 series routers.

# t1 external

To specify that a T1 channel on the Channelized T3 Interface Processor (CT3IP) in Cisco 7500 series routers is used as an external port so that the T1 channel can be further multiplexed on the Multichannel Interface Processor (MIP) or other multiplexing equipment, use the **t1 external** command in controller configuration mode. To remove a T1 as an external port, use the **no** form of this command.

```
t1 external channel [cablelength feet] [linecode [ami | b8zs]]
```

```
no t1 external channel
```

## Syntax Description

<b>channel</b>	Number 1, 2, or 3 that indicates the T1 channel.
<b>cablelength</b> <i>feet</i>	(Optional) Specifies the cable length, in feet, from the T1 channel to the external CSU or MIP. Values are from 0 to 655. Default is 133.
<b>linecode</b> <i>ami</i>   <i>b8zs</i>	(Optional) Specifies the line coding used by the T1. Values are alternate mark inversion (AMI) or bipolar 8 zero suppression (B8ZS). Default is B8ZS.

## Defaults

No external T1 is specified.  
The default cable length is 133 feet.  
The default line coding is B8ZS.

## Command Modes

Controller configuration

## Command History

Release	Modification
11.3	This command was introduced.

## Usage Guidelines

The first three T1 channels (1, 2, and 3) of the CT3IP can be broken out to the DSUP-15 connectors on the CPT3IP so that the T1 channel can be further demultiplexed by the MIP on the same router or on another router.

After you configure the external T1 channel, you can continue configuring it as a channelized T1 (also referred to as a *fractional* T1) from the MIP. All channelized T1 commands might not be applicable to the T1 interface. After you configure the channelized T1 on the MIP, you can continue configuring it as you would a normal serial interface. All serial interface commands might not be applicable to the T1 interface.

The line coding on the T1 channel and the MIP must be the same. Because the default line coding format on the T1 channel is B8ZS and the default line coding on the MIP is AMI, you must change the line coding on the MIP or on the T1 so that they match.

To determine if the external device connected to the external T1 port is configured and cabled correctly before configuring an external port, use the **show controllers t3** command and locate the line `Ext1...` in the display output. The line status can be one of the following:

- LOS—Loss of signal indicates that the port is not receiving a valid signal. This is the expected state if nothing is connected to the port.

- AIS—Alarm indication signal indicates that the port is receiving an all-ones signal.
- OK—A valid signal is being received and the signal is not an all-ones signal.

**Note**

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.

**Note**

Although you can specify a cable length from 0 to 655 feet, the hardware only recognizes the following ranges: 0 to 133, 134 to 266, 267 to 399, 400 to 533, and 534 to 655. For example, entering 150 feet uses the 134 to 266 range. If you later change the cable length to 200 feet, there is no change because 200 is within the 134 to 266 range. However, if you change the cable length to 399, the 267 to 399 range is used. The actual number you enter is stored in the configuration file.

**Examples**

The following example shows how to configure T1 1 on the CT3IP as an external port using AMI line coding and a cable length of 300 feet:

```
Router(config)# controllers t3 9/0/0
Router(config-controller)# t1 external 1 cablelength 300 linecode ami
```

**Related Commands**


Command	Description
<code>show controllers t3</code>	Displays the hardware and software driver information for a T3 controller.

# t1 fdl ansi

To enable the 1-second transmission of the remote performance reports via the Facility Data Link (FDL) per ANSI T1.403 for a T1 channel on the Channelized T3 Interface Processor (CT3IP) in Cisco 7500 series routers, use the **t1 fdl ansi** command in controller configuration mode. To disable the performance report, use the **no** form of this command.

**t1 channel fdl ansi**

**no t1 channel fdl ansi**

<b>Syntax Description</b>	<i>channel</i>	Number between 1 and 28 that indicates the T1 channel.
<b>Defaults</b>	Disabled	
<b>Command Modes</b>	Controller configuration	
<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	11.3	This command was introduced.
<b>Usage Guidelines</b>	<p>The <b>t1 fdl ansi</b> command can be used only if the T1 framing type is Extended Super Frame (ESF). To display the remote performance report information, use the <b>show controllers t3 remote performance</b> command.</p>	
 <b>Note</b>	<p>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.</p>	
<b>Examples</b>	<p>The following example shows how to generate the performance reports for T1 channel 8 on the CT3IP:</p> <pre>Router(config)# controller t3 9/0/0 Router(config-controller)# t1 8 fdl ansi</pre>	
<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<b>show controllers t3</b>	Displays the hardware and software driver information for a T3 controller.

# t1 framing

To specify the type of framing used by the T1 channels on the Channelized T3 Interface Processor (CT3IP) in Cisco 7500 series routers, use the **t1 framing** command in controller configuration mode.

**t1 channel framing {esf | sf}**

Syntax Description	
<i>channel</i>	Number between 1 and 28 that indicates the T1 channel.
<b>esf</b>	Specifies that Extended Super Frame (ESF) is used as the T1 framing type. This is the default.
<b>sf</b>	Specifies that Super Frame (SF) is used as the T1 framing type.

**Defaults** Extended Super Frame (ESF)

**Command Modes** Controller configuration

Command History	Release	Modification
	11.3	This command was introduced.

**Usage Guidelines** If you do not specify the **t1 framing** command, the default ESF is used.



**Note**

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.

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

**Examples** The following example shows how to set the framing for the T1 6 and T1 8 on the CT3IP to Super Frame:

```
Router(config)# controller t3 9/0/0
Router(config-controller)# t1 6 framing sf
Router(config-controller)# t1 8 framing sf
```

# t1 linecode

To specify the type of line coding used by the T1 channels on the Channelized T3 Interface Processor (CT3IP) in Cisco 7500 series routers, use the **t1 linecode** command in controller configuration mode.

**t1 channel linecode** [**ami** | **b8zs**]

Syntax Description	channel	Number between 1 and 28 that indicates the T1 channel.
	<b>ami</b>	Specifies that alternate mark inversion (AMI) line coding is used by the T1 channel.
	<b>b8zs</b>	Specifies that bipolar 8 zero suppression (B8ZS) line coding is used by the T1 channel. This is the default.

**Defaults** B8ZS

**Command Modes** Controller configuration

Command History	Release	Modification
	11.3	This command was introduced.

**Usage Guidelines** If you do not specify the **t1 linecode** command, the default B8ZS is used.

### AMI Line Coding

If you select **ami** line coding for the T1 channel, you must also invert the data on the T1 channel by using the **invert data** interface command. This is required because the T1 channel is bundled into the T3 signal, so there are no local T1 line drivers and receivers associated with it. Therefore, the **t1 channel linecode ami** command does not modify local line driver settings. Rather, it advises the CT3IP what line code the remote T1 is using. The CT3IP uses this information solely for the purpose of determining whether or not to enable the pulse density enforcer for that T1 channel.

### B8ZS Line Coding

When you select **b8zs** line coding, the pulse density enforcer is disabled. When you select **ami** line coding, the pulse density enforcer is enabled. To avoid having the pulse density enforcer corrupt data, the T1 channel should be configured for inverted data.



#### Note

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.

### Examples

The following example shows how to set the line coding for T1 channel 16 on the CT3IP to AMI:

```
Router(config)# controller t3 9/0/0
```

```
Router(config-controller)# t1 16 linecode ami
Router(config-controller)# exit
Router(config)# interface serial 9/0/0:16
Router(config-if)# invert data
```

**Related Commands**

Command	Description
<b>invert data</b>	Inverts the data stream.
<b>loopback remote (interface)</b>	Loops packets through a CSU/DSU, over a DS3 link or a channelized T1 link, to the remote CSU/DSU and back.

# t1 logging-events

To print typical T1 controller Up and Down messages on a channelized T3 port adapter in T3 controller, use the **t1 logging-events** command configuration mode. To disable printing of the T1 controller Up and Down messages, use the no form of this command.

**t1 {t1} logging-events [detail]**

**[no] t1 {t1} logging-events**

## Syntax Description

<i>t1</i>	Number between 1 and 28 that represents the T1 channel for the Channelized T3 Interface Processor (CT3IP) on Cisco 7500 series and Cisco 7200 series routers.
<b>detail</b>	(Optional) Enables printing the reason code when a T1 controller of a T3 controller changes from the Up state to the Down state.

## Defaults

The **t1 logging-events** command is the default.

## Command Modes

T3 controller configuration mode.

## Command History

Release	Modification
12.2(19c)	This command was introduced.

## Usage Guidelines

This command refers to the T1 controller as part of a T3 controller.

The **no t1 logging-events** command disables printing of the controller Up and Down messages. These messages will appear neither on the console nor in the logs.

## Examples

The following example uses the **t1 logging-events** command to print normal controller Up and Down messages, without indicating the reason code for a changed state. The T1 1 controller is part of the T3 controller with a bay/port of 4/1.

```
Router(config-controller)# t1 1 logging-events
```

```
*Jun 20 00:29:39: %CONTROLLER-5-UPDOWN: Controller T3 4/1 T1 1, changed state to UP
*Jun 20 00:30:09: %CONTROLLER-5-UPDOWN: Controller T3 4/1 T1 1, changed state to DOWN
```

The following example uses the **t1 logging-events detail** command to show the Out-of-Frame (OOF) reason code when the T1 1 controller of a T3 controller with a bay/port of 4/1 changes from an Up state to a Down state:

```
Router(config-controller)# t1 1 logging-events detail
```

```
*Jun 19 17:47:50: %CONTROLLER-5-DOWNDDETAIL: Controller T3 4/1 T1 1, changed state to down
due to OOF
```

Related Commands	Command	Description
	<a href="#">logging-events</a>	Prints typical T3 controller Up and Down messages on a channelized T3 port adapter.

# t1 test

To break out a T1 channel on the Channelized T3 Interface Processor (CT3IP) in Cisco 7500 series routers to the test port for testing, use the **t1 test** command in controller configuration mode. To remove the T1 channel from the test port, use the **no** form of this command.

```
t1 test channel [cablelength feet] [linecode [ami | b8zs]]
```

```
no t1 test channel
```

## Syntax Description

<i>channel</i>	Number between 1 and 28 that indicates the T1 channel.
<b>cablelength</b> <i>feet</i>	(Optional) Specifies the cable length, in feet, from the T1 channel to the external CSU or Multi-Channel Interface Processor (MIP). Values are from 0 to 655. Default is 133.
<b>linecode</b> { <b>ami</b>   <b>b8zs</b> }	(Optional) Specifies the line coding format used by the T1 channel. Values are alternate mark inversion (AMI) or bipolar 8 zero suppression (B8ZS). Default is B8ZS.

## Defaults

No test port is configured.  
The default cable length is 133 feet.  
The default line coding is B8ZS.

## Command Modes

Controller configuration

## Command History

Release	Modification
11.3	This command was introduced.

## Usage Guidelines

You can use the T1 test port available on the CT3IP to break out any of the 28 T1 channels for testing (for example, 24-hour bit error-rate tester (BERT) testing as is commonly done by telephone companies before a line is brought into service).

The T1 test port is also available as an external port. For more information on configuring an external port, see the **t1 external** controller configuration command.

To determine if the external device connected to the T1 test port is configured and cabled correctly before configuring a test port, use the **show controllers t3** command and locate the line `Ext1...` in the display output. The line status can be one of the following:

- LOS—Loss of signal indicates that the port is not receiving a valid signal. This is the expected state if nothing is connected to the port.
- AIS—Alarm indication signal indicates that the port is receiving an all-ones signal.
- OK—A valid signal is being received and the signal is not an all-ones signal.

**Note**

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.

**Note**

Although you can specify a cable length from 0 to 655 feet, the hardware only recognizes the following ranges: 0 to 133, 134 to 266, 267 to 399, 400 to 533, and 534 to 655. For example, entering 150 feet uses the 134 to 266 range. If you later change the cable length to 200 feet, there is no change because 200 is within the 134 to 266 range. However, if you change the cable length to 399, the 267 to 399 range is used. The actual number you enter is stored in the configuration file.

**Examples**

The following example shows how to configure T1 6 on the CT3IP as a test port using the default cable length and line coding:

```
Router(config)# controller t3 9/0/0
Router(config-controller)# t1 test 6
```

**Related Commands**

Command	Description
<code>show controllers t3</code>	Displays the hardware and software driver information for a T3 controller.
<code>t1 external</code>	Specifies that a T1 channel on the CT3IP in Cisco 7500 series routers is used as an external port so the T1 channel can be further multiplexed on the MIP or other multiplexing equipment.

# t1 timeslot

To specify the time slots and data rate used on each T1 channel on the Channelized T3 Interface Processor (CT3IP) in Cisco 7500 series routers, use the **t1 timeslot** command in controller configuration mode. To remove the configured T1 channel, use the **no** form of this command.

```
t1 channel timeslot range [speed {56 | 64}]
```

```
no t1 channel timeslot
```

## Syntax Description

<i>channel</i>	Number between 1 and 28 that indicates the T1 channel.
<i>range</i>	Specifies the time slots assigned to the T1 channel. The range can be from 1 to 24. A dash represents a range of time slots, and a comma separates time slots. For example, 1-10,15-18 assigns time slots 1 through 10 and 15 through 18.
<b>speed {56   64}</b>	(Optional) Specifies the data rate for the T1 channel, in kbps. Values are 56 or 64. The default is 64. The 56-kbps speed is valid only for T1 channels 21 through 28.

## Defaults

No time slots are specified for the T1 channel.  
The default data rate is 64 kbps.

## Command Modes

Controller configuration

## Command History

Release	Modification
11.3	This command was introduced.

## Usage Guidelines

You must specify the time slots used by each T1 channel.



### Note

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.

## Examples

The following example shows how to assign time slots 1 through 24 to T1 1 for full T1 bandwidth usage:

```
Router(config)# controller t3 9/0/0
Router(config-controller)# t1 1 timeslot 1-24
```

The following example shows how to assign time slots 21 to 23 and 26 to 28 and a data rate of 56 kbps to T1 6 for fractional T1 bandwidth usage:

```
Router(config)# controller t3 9/0/0
Router(config-controller)# t1 6 timeslot 21-23,26-28 speed 56
```

# t1 yellow

To enable detection and generation of yellow alarms for a T1 channel on the Channelized T3 Interface Processor (CT3IP) in Cisco 7500 series routers, use the **t1 yellow** command in controller configuration mode. To disable the detection and generation of yellow alarms, use the **no** form of this command.

```
t1 channel yellow {detection | generation}
```

```
no t1 channel yellow {detection | generation}
```

## Syntax Description

<i>channel</i>	Number between 1 and 28 that indicates the T1 channel.
<b>detection</b>	Detects yellow alarms. This is the default, along with <b>generation</b> .
<b>generation</b>	Generates yellow alarms. This is the default, along with <b>detection</b> .

## Defaults

Yellow alarms are detected and generated on the T1 channel.

## Command Modes

Controller configuration

## Command History

Release	Modification
11.3	This command was introduced.

## Usage Guidelines

If the T1 framing type is super frame (SF), you should consider disabling yellow alarm detection because the yellow alarm can be incorrectly detected with SF framing.



### Note

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.

## Examples

The following example shows how to disable the yellow alarm detection on T1 channel 6 on the CT3IP:

```
Router(config)# controller t3 9/0/0
Router(config-controller)# t1 6 framing sf
Router(config-controller)# no t1 6 yellow detection
```

# test aim eeprom

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

## test aim eeprom

**Syntax Description** This command has no arguments or keywords.

**Defaults** No tests are performed on the data compression AIM card.

**Command Modes** Privileged EXEC

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

**Table 101 Questions and Responses for test aim eeprom Command**

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 <b>test aim eeprom</b> command dialog. The AIM slot number chosen is displayed, and the default command is the last command entered.

**Table 101** Questions and Responses for test aim eeprom Command

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:

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

**test interface fastethernet** *number*

<b>Syntax Description</b>	<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 <b>show interfaces</b> command.
---------------------------	---------------	---

<b>Command Modes</b>	User EXEC Privileged EXEC
----------------------	------------------------------

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	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.

**Examples** The following example shows how to test a Fast Ethernet interface on a Cisco 4500 router:

```
Router# test interface fastethernet 0
```

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<b>ping (privileged)</b>	Diagnoses basic network connectivity on AppleTalk, CLNS, DECnet, IP, or Novell IPX networks.
	<b>ping (user)</b>	Provides simple ping diagnostics of network connectivity.
	<b>show interfaces</b>	Displays information about interfaces.

# test satellite satellite mfg link

To force the Cisco IP VSAT satellite WAN network module (NM-1VSAT-GILAT) to show that the backbone link to the hub is up, even when the link is actually down, use the **test satellite satellite mfg link** command in privileged EXEC mode.

```
test satellite satellite slot/unit mfg link {force | normal}
```

Syntax Description	slot	Router chassis slot in which the network module is installed.
	unit	Interface number. For NM-1VSAT-GILAT network modules, always use 0.
	force	Forces the satellite link to appear to be UP.
	normal	Allows the satellite link to display the actual status, UP or DOWN. This is the default.

**Defaults** The actual status (UP or DOWN) of the satellite link is displayed.

**Command Modes** Privileged EXEC

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

**Usage Guidelines** Use the **test satellite satellite mfg link** command only when instructed to do so by your satellite service provider or a technical support representative.

**Examples** The following example shows how to force the NM-1VSAT-GILAT network module to show that the backbone link to the hub is up, even if the link is actually down:

```
Router# test satellite satellite 1/0 mfg link force
```

The following example shows how to allow the NM-1VSAT-GILAT network module to show the actual status (UP or DOWN) of the satellite link:

```
Router# test satellite satellite 1/0 mfg link normal
```

# test satellite satellite reset

To reset the Cisco IP VSAT satellite WAN network module (NM-1VSAT-GILAT), use the **test satellite satellite reset** command in privileged EXEC mode.

**test satellite satellite *slot/unit* reset [hard]**

Syntax Description	slot	Router chassis slot in which the network module is installed.
	unit	Interface number. For NM-1VSAT-GILAT network modules, always use 0.
	hard	(Optional) Initiates a hardware reset. Not available on all routers.

**Defaults** Without the **hard** keyword, the command initiates a software reset.

**Command Modes** Privileged EXEC

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

**Usage Guidelines** Use the **test satellite satellite reset** command only when instructed to do so by your satellite service provider or a technical support representative. You will lose satellite network connectivity while the NM-1VSAT-GILAT network module resets.

We recommend that you first try a software reset. The hardware reset option is not available on all routers.

**Examples** The following example shows how to initiate a software reset of the NM-1VSAT-GILAT network module:

```
Router# test satellite satellite 1/0 reset
```

The following example shows how to initiate a hardware reset of the NM-1VSAT-GILAT network module:

```
Router# test satellite satellite 1/0 reset hard
```

# 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 mode.

**test service-module** *interface-type interface-number*

## Syntax Description

<i>interface-type</i>	Interface type.
<i>interface-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

The following example shows how to perform 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
<b>channelized</b>	Clears the interface counters.
<b>clear service-module serial</b>	Resets an integrated CSU/DSU.
<b>show service-module serial</b>	Displays the performance report for an integrated CSU/DSU.

# test trunk

To configure the test port on a trunk card, use the **test trunk** command in privileged EXEC mode.

```
test trunk stm1 { drop | monitor } { tx | rx } { on | off } e1 controller
```

## Syntax Description

<b>stm1</b>	Specifies the test port on an STM-1 trunk card. This keyword is supported only on the Cisco AS5850 platform.
<b>drop</b>	Specifies drop mode where the existing signal is dropped and the signal from the test port is sent to the controller.
<b>monitor</b>	Specifies monitor mode where the signal from the specified E1 controller is monitored via the test port. The original signal is not disturbed.
<b>tx</b>	Specifies that signal is sent on the transmit line.
<b>rx</b>	Specifies that signal is sent on the receive line.
<b>on</b>	Switches the test port on.
<b>off</b>	Switches the test port off.
<b>e1</b>	Specifies that an E1 controller is to be used for testing.
<i>controller</i>	Slot and port numbers to identify the E1 controller.

## Defaults

The test port is disabled.

## Command Modes

Privileged EXEC

## Command History

Release	Modification
11.0	This command was introduced.
12.2(15)T	The <b>stm-1</b> keyword was added.

## Usage Guidelines

If a controller does not go up, or there are a large number of errors associated with a specific E1 controller, you might be able to determine whether the problem is in the server card or in an external line by using the test port. The test port is located on the front panel of the SDH/STM-1 trunk card.

This command does not have a **no** form because the command itself switches the test port on or off.

To use this command, one E1 controller is selected and the transmit and receive lines can be put into drop or monitor mode. Both drop and monitor modes can be used at the same time on either the transmit or receive lines, but both transmit and receive lines cannot be used in drop or monitor mode at the same time.

## Examples

The following example shows how to configure a test port to use drop mode on the receive line of an E1 controller in the second path of an STM-1 trunk card in slot 2 of a Cisco AS5850 chassis:

```
Router# test trunk stm-1 drop rx on E1 2/0.2/1/2
```

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

## 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 thirty-two 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 shows how to enable framed mode on a serial interface on a G.703 E1 port adapter or an E1-G.703/G.704 port adapter:

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

**Related Commands**

<b>Command</b>	<b>Description</b>
<a href="#">ts16</a>	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
<b>fair-queue (WFQ)</b>	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 internally generated clock, use the **no** form of this command.

**transmit-clock-internal**

**no transmit-clock-internal**

**Syntax Description** This command has no arguments or keywords.

**Defaults** The internally generated clock is disabled.

**Command Modes** Interface configuration

Command History	Release	Modification
	10.0	This command was introduced.

**Examples** The following example shows how to enable the internally generated clock on serial interface 3/0 on a Cisco 7200 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**

<b>Syntax Description</b>	<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 from 0 to 131071. Default is 0.
---------------------------	--------------	--

<b>Defaults</b>	0 flags or microseconds
-----------------	-------------------------

<b>Command Modes</b>	Interface configuration
----------------------	-------------------------

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	10.0	This command was introduced.

<b>Usage Guidelines</b>	<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>
-------------------------	--

<b>Examples</b>	The following example shows how to specify a delay of 300 microseconds on serial interface 0:
-----------------	---

```
Router(config)# interface serial 0
Router(config-if)# transmitter-delay 300
```

# ts16

To control the use of time slot 16 for data on a G.703 E1 interface or on an 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 implemented on 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 shows how to configure time slot 16 to be used for data on a G.703 E1 interface or an E1-G.703/G.704 serial port adapter:

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

Related Commands	Command	Description
	<a href="#">timeslot</a>	Enables framed mode serial interface on a G.703 E1 port adapter, an FSIP, or an E1-G.703/G.704 serial port adapter.

# tug-2 e1

To create E1 controllers for a specified path under the Tributary Unit group type 2 (TUG-2), use the **tug-2 e1** command in controller configuration mode.

```
tug-2 tug-2-number e1 e1-number
```

## Syntax Description

<i>tug-2-number</i>	Number, or range of numbers, from 1 to 7. To specify a range of TUG-2 numbers use a dash between the values, for example 1-5. An individual TUG-2 can be specified using a comma between values, for example 2,4. Default is 1.
<i>e-1-number</i>	Number, or range of numbers, from 1 to 3. To specify a range of E1 numbers use a dash between the values, for example 1-3. An individual E1 can be specified using a comma between values, for example 2,3.

## Defaults

Default *tug-2-number* value for STM-1 card is 1.

## Command Modes

Controller configuration

## Command History

Release	Modification
12.0(14)S	This command was introduced.
12.2(15)T	This command was integrated into Cisco IOS Release 12.2(15)T.

## Usage Guidelines

Use the **tug-2 e1** command to create an E1 controller with the following name format:

```
slot/port.path/tug-2-number/e1-number
```

Up to 21 controllers can be created for one path. Only one path can be selected at a time.

## Examples

The following example shows how to configure 15 E1 controllers on the second path of an STM-1 in physical slot number 2 of a Cisco AS5850 chassis:

```
Router(config)# controller sonet 2/0
Router(config-controller)# aug mapping au-4
Router(config-ctrlr-tug3)# au-4 1 tug-3 2
Router(config-ctrlr-tug3)# tug-2 5 e1 3
```

## Related Commands

Command	Description
<b>show controller sonet</b>	Displays information about SONET controllers.

# tunnel bandwidth

To set the transmit bandwidth used by the tunnel interface, use the **tunnel bandwidth** command in interface configuration mode. To restore the default setting, use the **no** form of this command.

**tunnel bandwidth** { **receive** | **transmit** } *bandwidth*

**no tunnel bandwidth**

## Syntax Description

<b>receive</b>	Specifies the bandwidth to be used to receive packets through the tunnel. <b>Note</b> This keyword is no longer used and will be removed in future releases.
<b>transmit</b>	Specifies the bandwidth to be used to send packets through the tunnel.
<i>bandwidth</i>	Bandwidth, in kbps. Range is from 0 to 2147483647. Default is 8000.

## Defaults

8000 kbps

## Command Modes

Interface configuration

## Command History

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

## Usage Guidelines

Use the **tunnel bandwidth** command to specify the capacity of the satellite link.

## Examples

The following example shows how to set the satellite tunnel bandwidth to 1000 kbps for transmitting packets using Rate Based Satellite Control Protocol:

```
Router(config)# interface tunnel 0
Router(config-if)# tunnel bandwidth transmit 1000
```

## Related Commands

Command	Description
<b>tunnel destination</b>	Specifies the destination for a tunnel interface.
<b>tunnel mode</b>	Sets the encapsulation mode for a tunnel interface.
<b>tunnel source</b>	Sets the source address of a tunnel interface.

# 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

---

<b>Release</b>	<b>Modification</b>
10.0	This command was introduced.

---

---

**Usage Guidelines** This command currently applies to generic routing 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** The following example shows how to enable encapsulator-to-decapsulator checksumming of packets for all protocols on the tunnel interface:

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

# 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 4294967295 that identifies the tunnel key.
-------------------	---

## Defaults

No tunnel ID keys are enabled.

## 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 shows how to set the tunnel ID 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 ipv6 | gre multipoint | ipip
             [decapsulate-any] | ipsec ipv4 | iptalk | ipv6 | mpls | nos | rbscp}
```

```
no tunnel mode
```

## Syntax Description

<b>aurp</b>	AppleTalk Update-Based Routing Protocol.
<b>cayman</b>	Cayman TunnelTalk AppleTalk encapsulation.
<b>decapsulate-any</b>	(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.
<b>dvmrp</b>	Distance Vector Multicast Routing Protocol.
<b>eon</b>	EON compatible CLNS tunnel.
<b>gre</b>	Generic routing encapsulation protocol. This is the default.
<b>gre ipv6</b>	GRE tunneling using IPv6 as the delivery protocol.
<b>gre multipoint</b>	Multipoint GRE (mGRE).
<b>ipip</b>	IP-over-IP encapsulation.
<b>ipsec ipv4</b>	Tunnel mode is <b>ipsec</b> and the transport is IPv4.
<b>iptalk</b>	Apple IPTalk encapsulation.
<b>ipv6</b>	Static tunnel interface configured to encapsulate IPv6 or IPv4 packets in IPv6.
<b>mpls</b>	Multiprotocol Label Switching encapsulation.
<b>nos</b>	KA9Q/NOS compatible IP over IP.
<b>rbscp</b>	Rate Based Satellite Control Protocol (RBSCP).

## Defaults

GRE tunneling (**gre**)

## 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"> <li>• <b>aurp</b></li> <li>• <b>dvmrp</b></li> <li>• <b>ipip</b></li> </ul>
11.2	The optional <b>decapsulate-any</b> keyword was added.
12.2(13)T	The <b>gre multipoint</b> keyword was added.

Release	Modification
12.3(7)T	The following keywords were added: <ul style="list-style-type: none"> <li>• <b>gre ipv6</b> to support GRE tunneling using IPv6 as the delivery protocol.</li> <li>• <b>ipv6</b> to allow a static tunnel interface to be configured to encapsulate IPv6 or IPv4 packets in IPv6.</li> <li>• <b>rbscp</b> to support Rate Based Satellite Control Protocol (RBSCP).</li> </ul>
12.3(14)T	The <b>ipsec ipv4</b> keyword was added to support IPSec virtual tunnel interfaces.

## 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 the GRE interface are supported only on point-to-point GRE tunnels.

### RBSCP

RBSCP tunneling is designed for wireless or long-distance delay links with high error rates, such as satellite links. Using tunnels, RBSCP can improve the performance of certain IP protocols, such as TCP and IPSec, over satellite links without breaking the end-to-end model.

**Examples****Cayman Tunneling**

The following example shows how to enable 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 shows how to enable 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
```

**IPSec in IPv4 Transport**

The following example shows how to configure a tunnel using IPSec encapsulation with IPv4 as the transport mechanism.

```
Router(config)# crypto ipsec profile PROF
Router(config)# set transform tset
!
Router(config)# interface tunnel0
Router(config-if)# ip address 1.1.1.1 255.255.255.0
Router(config-if)# tunnel mode ipsec ipv4
Router(config-if)# tunnel source Loopback0
Router(config-if)# tunnel destination 172.16.1.1
Router(config-if)# tunnel protection ipsec profile PROF
```

**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 that 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
```

**RBSCP Tunneling**

The following example shows how to enable RBSCP 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 rbscp
```

Related Commands	Command	Description
	<b>appletalk cable-range</b>	Enables an extended AppleTalk network.
	<b>appletalk zone</b>	Sets the zone name for the connected AppleTalk network.
	<b>tunnel destination</b>	Specifies the destination for a tunnel interface.
	<b>tunnel protection</b>	Associates a tunnel interface with an IPSec profile.
	<b>tunnel source</b>	Sets the source address of a tunnel interface.

# tunnel path-mtu-discovery

To enable Path MTU Discovery (PMTUD) on a generic routing encapsulation (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**} | **min-mtu** *mtu-bytes*]

**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"> <li><i>aging-mins</i>—Number of minutes. Range is from 10 to 30. Default is 10.</li> <li><b>infinite</b>—Disables the age timer.</li> </ul>	
	min-mtu	(Optional) Specifies the minimum Path MTU across GRE tunnels.
	<ul style="list-style-type: none"> <li><i>mtu-bytes</i>—Number of bytes. Range is from 92 to 65535. Default is 92.</li> </ul>	

**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.
	12.2(13)T	The <b>min-mtu</b> keyword and <i>mtu-bytes</i> argument were added.

**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 Internet Control Message Protocol (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.

The *min-mtu* argument sets a low limit on the MTU that can be learned via the PMTUD process. Any ICMP signaling received specifying an MTU less than the minimum MTU configured will be ignored. This feature can be used to prevent a denial of service attack from any node that can send a specially crafted ICMP message to the router, specifying a very small MTU. For more information, see “*Crafted ICMP Messages Can Cause Denial of Service*” at the following URL:

[http://www.cisco.com/en/US/products/products\\_security\\_advisory09186a0080436587.shtml](http://www.cisco.com/en/US/products/products_security_advisory09186a0080436587.shtml)



#### 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 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
<b>interface</b>	Configures an interface and enters interface configuration mode.
<b>show interfaces tunnel</b>	Displays information about the specified tunnel interface.

# tunnel protection

To associate a tunnel interface with an IP Security (IPSec) profile, use the **tunnel protection** command in interface configuration mode. To disassociate a tunnel with an IPSec profile, use the **no** form of this command.

**tunnel protection ipsec profile** *name* [**shared**]

**no tunnel protection ipsec profile** *name* [**shared**]

Syntax Description		
	<b>ipsec profile</b>	Enables generic routing encapsulation (GRE) tunnel encryption via IPSec.
	<i>name</i>	Name of the IPSec profile. This value must match the <i>name</i> specified in the <b>crypto ipsec profile</b> command.
	<b>shared</b>	(Optional) Allows the tunnel protection IPSec Security Association Database (SADB) to share the same dynamic crypto map instead of creating a unique crypto map per tunnel interface.  <b>Note</b> Unlike the <b>tunnel protection</b> command, which specifies that IPSec encryption will be performed after GRE encapsulation, configuring a crypto map on a tunnel interface specifies that encryption will be performed before GRE encapsulation.

**Defaults** Tunnel interfaces are not associated with IPSec profiles.

**Command Modes** Interface configuration

Command History	Release	Modification
	12.2(13)T	This command was introduced.
	12.3	The <b>shared</b> keyword was added.

**Usage Guidelines** Use the **tunnel protection** command to specify that IPSec encryption will be performed after the GRE has been added to the tunnel packet. The **tunnel protection** command can be used with multipoint GRE (mGRE) and point-to-point GRE (p-pGRE) tunnels. With p-pGRE tunnels, the tunnel destination address will be used as the IPSec peer address. With mGRE tunnels, multiple IPSec peers are possible; the corresponding Next Hop Resolution Protocol (NHRP) mapping nonbroadcast multiaccess (NBMA) destination addresses will be used as the IPSec peer addresses.

### The shared Keyword

If you wish to configure two Dynamic Multipoint VPN (DMVPN) mGRE and IPSec tunnels on the same router, you *must* issue the **shared** keyword.

The dynamic crypto map that is created by the **tunnel protection** command is always different from a crypto map that is configured directly on the interface.

**Note**

GRE tunnel keepalives (configured with the **keepalive** command under the GRE interface) are not supported in combination with the **tunnel protection** command.

**Examples**

The following example shows how to associate the IPsec profile “vpnprof” with an mGRE tunnel interface. In this example, the IPsec source peer address will be the IP address from Ethernet interface 0. There is a static NHRP mapping from IP address 10.0.0.3 to IP address 172.16.2.1, so for this NHRP mapping the IPsec destination peer address will be 172.16.2.1. The IPsec proxy will be as follows: **permit gre host ethernet0-ip-address host ip-address**. Other NHRP mappings (static or dynamic) will automatically create additional IPsec security associations (SAs) with the same source peer address and the destination peer address from the NHRP mapping. The IPsec proxy for these NHRP mappings will be as follows: **permit gre host ethernet0-ip-address host NHRP-mapping-NBMA-address**.

```
crypto ipsec profile vpnprof
  set transform-set trans2
!
interface Tunnel0
  bandwidth 1000
  ip address 10.0.0.1 255.255.255.0
! Ensures that longer packets are fragmented before they are encrypted; otherwise, the
! receiving router would have to do the reassembly.
  ip mtu 1416
  ip nhrp authentication donttell
  ip nhrp map multicast dynamic
  ip nhrp network-id 99
  ip nhrp holdtime 300
! 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 the IPsec peer address to the 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
```

The following example shows how to associate the IPsec profile “vpnprof” with a p-pGRE tunnel interface. In this example, the IPsec source peer address will be the IP address from Ethernet interface 0. The IPsec destination peer address will be 172.16.1.10 (per the **tunnel destination address** command). The IPsec proxy will be as follows: **permit gre host ethernet0-ip-address host ip-address**.

```
interface Tunnel1
  ip address 10.0.1.1 255.255.255.252
! Ensures that longer packets are fragmented before they are encrypted; otherwise, the
! receiving router would have to do the reassembly.
  ip mtu 1420
  tunnel source Ethernet0
  tunnel destination 172.16.1.10
  tunnel protection ipsec profile vpnprof
```

**Related Commands**

<b>Command</b>	<b>Description</b>
<b>crypto ipsec profile</b>	Defines the IPSec parameters that are to be used for IPSec encryption between two IPSec routers.
<b>interface</b>	Configures an interface type and enters interface configuration mode.
<b>keepalive (tunnel interfaces)</b>	Enables keepalive packets and specifies the number of times that the Cisco IOS software tries to send keepalive packets without a response before bringing the tunnel protocol down for a specific interface.
<b>permit</b>	Sets conditions for a named IP access list.

# tunnel rbscp ack\_split

To enable TCP acknowledgement (ACK) splitting for Rate Based Satellite Control Protocol (RBSCP) tunnels, use the **tunnel rbscp ack\_split** command in interface configuration mode. To disable TCP acknowledgement splitting for RBSCP tunnels, use the **no** form of this command.

**tunnel rbscp ack\_split** *split-size*

**no tunnel rbscp ack\_split** *split-size*

## Syntax Description

<i>split-size</i>	Number of ACKs to send for every ACK received. Range is from 1 to 32. Default is 4.
-------------------	---

## Defaults

TCP acknowledgement splitting for RBSCP tunnels is disabled.

## Command Modes

Interface configuration

## Command History

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

## Usage Guidelines

Performance improvements can be made for clear-text TCP traffic using ACK splitting where a number of additional TCP ACKs are generated for each TCP ACK received. TCP will open a congestion window by one maximum transmission unit (MTU) for each TCP ACK received. Opening the congestion window results in increased bandwidth becoming available. Use the **tunnel rbscp ack\_split** command only when the satellite link is not using all the available bandwidth. Encrypted traffic cannot use ACK splitting.

## Examples

The following example shows how to enable RBSCP tunnel TCP ACK splitting and configure three ACK packets to be sent for each ACK packet received:

```
Router(config)# interface tunnel 0
Router(config-if)# tunnel rbscp ack_split 3
```

## Related Commands

Command	Description
<b>show rbscp</b>	Displays state and statistical information about RBSCP tunnels.

# tunnel rbscp delay

To enable the Rate Based Satellite Control Protocol (RBSCP) tunnel delay, use the **tunnel rbscp delay** command in interface configuration mode. To disable RBSCP tunnel delay, use the **no** form of this command.

**tunnel rbscp delay**

**no tunnel rbscp delay**

**Syntax Description** This command has no arguments or keywords.

**Defaults** RBSCP tunnel delay is disabled.

**Command Modes** Interface configuration

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

**Usage Guidelines** Use the **tunnel rbscp delay** command only if the RBSCP tunnel has a round-trip time (RTT) over 700 milliseconds.

**Examples** The following example shows how to enable the RBSCP tunnel delay:

```
Router(config)# interface tunnel 0  
Router(config-if)# tunnel rbscp delay
```

Command	Description
<b>show rbscp</b>	Displays state and statistical information about RBSCP tunnels.

# tunnel rbscp input\_drop

To configure the input queue size on a Rate Based Satellite Control Protocol (RBSCP) tunnel, use the **tunnel rbscp input\_drop** command in interface configuration mode. To restore the default input queue size, use the **no** form of this command.

**tunnel rbscp input\_drop** *bw-delay-products*

**no tunnel rbscp input\_drop**

## Syntax Description

<i>bw-delay-products</i>	Number of bandwidth delay products (BDP) bytes that can be queued before packets are dropped on the input side. Range from 1 to 10. Default is 2.
--------------------------	---

## Defaults

Input queue size is 2 BDP bytes.

## Command Modes

Interface configuration

## Command History

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

## Usage Guidelines

Use the **tunnel rbscp input\_drop** command to restrict the amount of data queued by the router. After the configured byte limit is reached, packets that would be encapsulated and sent via the tunnel are dropped on the input side. Congestion control of the satellite link is also provided by this command because the dropped packets will force the end hosts to reduce their sending rate of packets.

Use this command in conjunction with the **tunnel rbscp long\_drop** command which allows packets that are waiting in an RBSCP tunnel encapsulation queue to be dropped after a period of time.

## Examples

The following example shows how to set the RBSCP tunnel queue size to 5 BDP bytes:

```
Router(config)# interface tunnel 0
Router(config-if)# tunnel rbscp input_drop 5
```

## Related Commands

Command	Description
<b>show rbscp</b>	Displays state and statistical information about RBSCP tunnels.
<b>tunnel rbscp long_drop</b>	Allows packets to be dropped after waiting in the RBSCP tunnel encapsulation queue for too long.

# tunnel rbscp long\_drop

To allow packets to be dropped that have been queued too long for Rate Based Satellite Control Protocol (RBSCP) tunnel encapsulation, use the **tunnel rbscp long\_drop** command in interface configuration mode. To disable the dropping of queued packets, use the **no** form of this command.

**tunnel rbscp long\_drop**

**no tunnel rbscp long\_drop**

## Syntax Description

This command has no arguments or keywords.

## Defaults

No queued packets are dropped.

## Command Modes

Interface configuration

## Command History

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

## Usage Guidelines

The **tunnel rbscp long\_drop** command allows the transmitting router to drop packets that have been waiting in the queue for RBSCP tunnel encapsulation for a long time. The period of time after which packets are dropped is determined using the round-trip time (RTT) estimate of the tunnel.

Use this command in conjunction with the **tunnel rbscp input\_drop** command which configures the size of the input queue. After the configured byte limit of the input queue is reached, packets are dropped.

## Examples

The following example shows how to allow packets to be dropped when they have been queued for RBSCP tunnel encapsulation too long:

```
Router(config)# interface tunnel 0
Router(config-if)# tunnel rbscp long_drop
```

## Related Commands

Command	Description
<b>show rbscp</b>	Displays state and statistical information about RBSCP tunnels.
<b>tunnel rbscp input_drop</b>	Configures the input queue size on an RBSCP tunnel.

# tunnel rbscp report

To report dropped Rate Based Satellite Control Protocol (RBSCP) packets to the Stream Control Transmission Protocol (SCTP), use the **tunnel rbscp report** command in interface configuration mode. To disable dropped-packet reporting to SCTP, use the **no** form of this command.

**tunnel rbscp report**

**no tunnel rbscp report**

**Syntax Description** This command has no arguments or keywords.

**Defaults** RBSCP dropped-packet reporting is enabled.

**Command Modes** Interface configuration

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

**Usage Guidelines** Use the **tunnel rbscp report** command to provide early reporting of dropped RBSCP packets to SCTP instead of attempting retransmission of the packets at the router. SCTP will inform the end hosts of the dropped packets and allow the end hosts to retransmit the packets. Reporting dropped packets through SCTP provides better throughput because the packet dropping is not assumed to be caused by congestion.

**Examples** The following example shows how to disable the SCTP drop reporting (reporting is enabled by default):

```
Router(config)# interface tunnel 0
Router(config-if)# no tunnel rbscp report
```

Related Commands	Command	Description
	<b>show rbscp</b>	Displays state and statistical information about RBSCP tunnels.

# tunnel rbscp window\_stuff

To enable TCP window stuffing by increasing the value of the TCP window scale for Rate Based Satellite Control Protocol (RBSCP) tunnels, use the **tunnel rbscp window\_stuff** command in interface configuration mode. To restore the default TCP window scale value, use the **no** form of this command.

```
tunnel rbscp window_stuff step-size
```

```
no tunnel rbscp window_stuff
```

<b>Syntax Description</b>	<i>step-size</i>	Increment step size for the TCP window scale. Range is from 1 to 20. Default is 1.
---------------------------	------------------	--

<b>Defaults</b>	TCP window stuffing is disabled.
-----------------	----------------------------------

<b>Command Modes</b>	Interface configuration
----------------------	-------------------------

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	12.3(7)T	This command was introduced.

<b>Usage Guidelines</b>	Use the <b>tunnel rbscp window_stuff</b> command to make the sending host believe that the receiving host has a larger window by artificially increasing the TCP window size. RBSCP buffers the additional window and which be configured up to the satellite link bandwidth or the memory available on the router.
-------------------------	---



**Note**

The actual TCP window size value that is used by the router may be smaller than the configured value because of the available bandwidth.

<b>Examples</b>	The following example shows how to enable TCP window stuffing on the RBSCP tunnel and configure a window size of 2:
-----------------	---

```
Router(config)# interface tunnel 0
Router(config-if)# tunnel rbscp window_stuff 2
```

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<b>show rbscp</b>	Displays state and statistical information about RBSCP tunnels.

# 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 routing 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 shows how to configure the tunnel to drop datagrams that arrive out of order:

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

# tunnel vrf

To associate a VPN routing and forwarding (VRF) instance with a specific tunnel destination, interface or subinterface, use the **tunnel vrf** command in global configuration mode or interface configuration mode. To disassociate a VRF from the tunnel destination, use the no form of this command.

**tunnel vrf** *vrf-name*

**no tunnel vrf** *vrf-name*

## Syntax Description

<i>vrf-name</i>	Name assigned to a VRF.
-----------------	-------------------------

## Defaults

The default destination is determined by the global routing table.

## Command Modes

Global configuration  
Interface configuration

## Command History

Release	Modification
12.0(23)S	This command was introduced.
12.3(2)T	This command was integrated into Cisco IOS Release 12.3(2)T.

## Usage Guidelines

The tunnel source and destination must be in the same VRF.

Either the IP VRF or the tunnel VRF can be set to the global routing table (using the **no ip vrf forwarding** *vrf* command or the **no tunnel vrf** *vrf* command).

The tunnel will be disabled if no route to the tunnel destination is defined. If the tunnel VRF is set, there must be a route to that destination in the VRF.

## Examples

The following example shows how to associate a VRF with a tunnel destination. The tunnel endpoint, 10.5.5.5 will be looked up in the blue VRF.

```
interface tunnel0
 ip vrf forwarding green
 ip address 10.3.3.3 255.255.255.0
 tunnel source loop 0
 tunnel destination 10.5.5.5
 tunnel vrf blue
```

## Related Commands

Command	Description
<b>ip route vrf</b>	Establishes static routes for a VRF.
<b>ip vrf</b>	Configures a VRF routing table.
<b>ip vrf forwarding</b>	Associates a VPN VRF instance with an interface or subinterface.

<b>Command</b>	<b>Description</b>
<b>tunnel destination</b>	Specifies the destination for a tunnel interface.
<b>tunnel source</b>	Sets the source address for a tunnel interface.

# tx-queue-limit

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

**tx-queue-limit** *number*

<b>Syntax Description</b>	<i>number</i>	Maximum number of transmit buffers that the specified interface can subscribe.
<b>Defaults</b>	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 <b>show controllers mci</b> command.	
<b>Command Modes</b>	Interface configuration	
<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	10.0	This command was introduced.
<b>Usage Guidelines</b>	This command should be used only under the guidance of a technical support representative. This command does not have a <b>no</b> form.	
<b>Examples</b>	The following example shows how to set the maximum number of transmit buffers on the interface to 5:  Router(config)# <b>interface ethernet 0</b> Router(config-if)# <b>tx-queue-limit 5</b>	
<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<b>show controllers mci</b>	Displays all information under the MCI card or the SCI.

## xconnect (CEM)

To build one end of a circuit emulation (CEM) connection and to enter CEM xconnect configuration mode, use the **xconnect** command in CEM configuration mode. To remove any existing CEM connections from this CEM channel, use the **no** form of this command.

**xconnect** *remote-ip-address* *virtual-connect-ID* **encapsulation** *encapsulation-type*

**no xconnect**

### Syntax Description

<i>remote-ip-address</i>	IP address of an interface—physical or loopback—on the destination router.
<i>virtual-connect-ID</i>	Virtual connect ID (VCID). For CEM over IP (CEoIP), you must enter a value of 0.
<b>encapsulation</b>	Sets the encapsulation type.
<i>encapsulation-type</i>	Encapsulation type. You must set the encapsulation type to UDP.

### Defaults

No CEM connections are built.

### Command Modes

CEM configuration

### Command History

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

### Examples

The following example shows how to build one end of a CEoIP connection and to enter CEM xconnect configuration mode.

```
Router(config-cem)# xconnect 10.0.5.1 0 encapsulation udp
Router(config-cem-xconnect)#
```

### Related Commands

Command	Description
<b>cem</b>	Enters circuit emulation configuration mode.
<b>local ip address</b>	Defines the IP address of the local router.
<b>local udp port</b>	Defines the local UDP port.
<b>remote udp port</b>	Defines the UDP port of a remote endpoint.
<b>show cem</b>	Displays CEM channel statistics.

# yellow

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

**yellow** {**generation** | **detection**}

## Syntax Description

<b>generation</b>	Enables or disables generation of yellow alarms.
<b>detection</b>	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	This command was implemented on Cisco 7100 series routers.
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. If the received signal is lost the yellow alarm can be generated to indicate a frame loss event. Generation of a yellow alarm will ensure that the alarm is sent to the remote end of the link. When the remote end is transmitting a yellow alarm, detection must be enabled to detect the alarm condition.

## Examples

The following example shows how to enable 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
```