

## shutdown (controller)

To disable the Channelized T3 Interface Processor (CT3IP) in Cisco 7500 series routers, use the **shutdown** controller configuration command. To restart a disabled CT3IP, use the **no** form of this command.

**shutdown**  
**no shutdown**

### Syntax Description

This command has no arguments or keywords.

### Default

Enabled

### Command Mode

Controller configuration

### Usage Guidelines

This command first appeared in Cisco IOS Release 11.3.

Shutting down the CT3IP disables all functions on the interface and sends a blue alarm to the network. This command marks the interface as unavailable. To check if the CT3IP is disabled, use the **show controller t3** command.

### Example

In the following example, the CT3IP is shutdown:

```
controller t3 9/0/0
shutdown
```

### Related Commands

You can use the master indexes or search online to find documentation of related commands.

**show controllers t3**

## shutdown (hub configuration)

Use the **shutdown** hub configuration command to shut down a port on an Ethernet hub of a Cisco 2505 or Cisco 2507. Use the **no** form of this command to restart the disabled hub.

**shutdown**  
**no shutdown**

### Syntax Description

This command has no arguments or keywords.

### Command Mode

Hub configuration

### Usage Guidelines

This command first appeared in Cisco IOS Release 10.3.

### Example

The following example shuts down hub 0, ports 1 through 3:

```
hub ethernet 0 1 3
shutdown
```

### Related Commands

You can use the master indexes or search online to find documentation of related commands.

**hub**

## shutdown (interface)

To disable an interface, use the **shutdown** interface configuration command. To restart a disabled interface, use the **no** form of this command.

**shutdown**  
**no shutdown**

### Syntax Description

This command has no arguments or keywords.

### Default

Enabled

### Command Mode

Interface configuration

### Usage Guidelines

This command first appeared in Cisco IOS Release 10.0.

The **shutdown** command disables all functions on the specified interface. On serial interfaces, this command causes the DTR signal to be dropped. On Token Ring interfaces, this command causes the interface to be deinserted from the ring. On FDDI interfaces, this command causes the optical bypass switch, if present, to go into bypass mode.

This command also marks the interface as unavailable. To check whether an interface is disabled, use the EXEC command **show interfaces**. An interface that has been shut down is shown as administratively down in the display from this command.

### Examples

The following example turns off Ethernet interface 0:

```
interface ethernet 0
 shutdown
```

The following example turns the interface back on:

```
interface ethernet 0
 no shutdown
```

### Related Commands

You can use the master indexes or search online to find documentation of related commands.

**show interfaces**

## smt-queue-threshold

To set the maximum number of unprocessed FDDI station management (SMT) frames that will be held for processing, use the **smt-queue-threshold** global configuration command. Use the **no** form of this command to restore the queue to the default.

**smt-queue-threshold** *number*  
**no smt-queue-threshold**

### Syntax Description

*number* Number of buffers used to store unprocessed SMT messages that are to be queued for processing. Acceptable values are positive integers.

### Default

The default threshold value is equal to the number of FDDI interfaces installed in the router.

### Command Mode

Global configuration

### Usage Guidelines

This command first appeared in Cisco IOS Release 10.0.

This command helps ensure that the routers keep track of FDDI *upstream* and *downstream* neighbors, particularly when a router includes more than one FDDI interface.

In FDDI, upstream and downstream neighbors are determined by transmitting and receiving SMT Neighbor Information Frames (NIFs). The router can appear to lose track of neighbors when it receives an SMT frame and the queue currently contains an unprocessed frame. This occurs because the router discards incoming SMT frames if the queue is full. Discarding SMT NIF frames can cause the router to lose its upstream or downstream neighbor.

---

**Note** Use this command carefully, because the SMT buffer is charged to the inbound interface (input hold queue) until the frame is completely processed by the system. Setting this value to a high limit can impact buffer usage and the ability of the router to receive routable packets or routing updates.

---

### Example

The following example specifies that the SMT queue can hold ten messages. As SMT frames are processed by the system, the queue is decreased by one:

```
smt-queue-threshold 10
```

## snmp trap illegal-address

To issue an SNMP trap when a MAC address violation is detected on an Ethernet hub port of a Cisco 2505, Cisco 2507, or Cisco 2516 router, use the **snmp trap illegal-address** hub configuration command. Use the no form to disable this function.

```
snmp trap illegal-address
no snmp trap illegal-address
```

### Syntax Description

This command has no arguments or keywords.

### Default

No SNMP trap is issued.

### Command Mode

Hub configuration

### Usage Guidelines

This command first appeared in Cisco IOS Release 11.1.

In addition to setting the **snmp trap illegal-address** command on the Ethernet hub, you can set the frequency that the trap is sent to the network management station (NMS). This is done on the NMS via the Cisco Repeater MIB. The frequency of the trap can be configured for once only or at a decaying rate (the default). If the decaying rate is used, the first trap is sent immediately, the second trap is sent after one minute, the third trap is sent after two minutes, and so on until 32 minutes at which time the trap is sent every 32 minutes. If you use a decaying rate, you can also set the trap acknowledgment so the trap will be acknowledged after it is received and will no longer be sent to the network management station.

Because traps are not reliable, additional information on a port basis is provided by the Cisco Repeater MIB. The network management function can query the following information: the last illegal MAC source address, the illegal address trap acknowledgment, the illegal address trap enabled, the illegal address first heard (timestamp), the illegal address last heard (timestamp), the last illegal address trap count for the port, and the illegal address trap total count for the port.

In addition to issuing a trap when a MAC address violation is detected, the port is also disabled as long as the MAC address is invalid. The port is enabled and the trap is no longer sent when the MAC address is valid (that is, either the address was configured correctly or learned).

### Example

The following example enables an SNMP trap to be issued when a MAC address violation is detected on hub ports 2, 3, or 4. SNMP support must already be configured on the router.

```
hub ethernet 0 2 4
snmp trap illegal-address
```

### Related Commands

You can use the master indexes or search online to find documentation of related commands

**hub ethernet**

---

## source-address

To configure source address control on a port on an Ethernet hub of a Cisco 2505 or Cisco 2507, use the **source-address** hub configuration command. To remove a previously defined source address, use the **no** form of this command.

```
source-address [mac-address]  
no source-address
```

### Syntax Description

*mac-address* (Optional) MAC address in the packets that the hub will allow to access the network.

### Default

Disabled

### Command Mode

Hub configuration

### Usage Guidelines

This command first appeared in Cisco IOS Release 10.3.

If you omit the MAC address, the hub uses the value in the last source address register, and if the address register is invalid, it will remember the first MAC address it receives on the previously specified port, and allow only packets from that MAC address onto that port.

### Examples

The following example configures the hub to allow only packets from MAC address 1111.2222.3333 on port 2 of hub 0:

```
hub ethernet 0 2  
source-address 1111.2222.3333
```

The following example configures the hub to use the value of the last source address register. If the address register is invalid, it will remember the first MAC address it receives on port 2, and allow only packets from the learned MAC address on port 2:

```
hub ethernet 0 2  
source-address
```

### Related Commands

You can use the master indexes or search online to find documentation of related commands.

**hub**

## sqelch

To extend the Ethernet twisted-pair 10BaseT capability beyond the standard 100 meters on the Cisco 4000 platform, use the **sqelch** interface configuration command. To restore the default, use the **no** form of this command.

```
sqelch { normal | reduced }  
no sqelch { normal | reduced }
```

### Syntax Description

**normal**        Allows normal capability.

**reduced**      Allows extended 10BaseT capability.

### Default

Normal range

### Command Mode

Interface configuration

### Usage Guidelines

This command first appeared in Cisco IOS Release 10.0.

### Example

The following example extends the twisted-pair 10BaseT capability on the cable attached to Ethernet interface 2:

```
interface ethernet 2  
  sqelch reduced
```

## t1 bert

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

```
t1 channel bert pattern {0s | 1s | 2^15 | 2^20 | 2^23} interval minutes
no t1 channel bert pattern {0s | 1s | 2^15 | 2^20 | 2^23} interval minutes
```

### Syntax Description

<i>channel</i>	Number between 1 and 28 that indicates the T1 channel.
<b>pattern</b> {0s   1s   2^15   2^20   2^23}	Specifies the length of the repeating BERT test pattern. Values are: <ul style="list-style-type: none"> <li>0s—Repeating pattern of zeros (...000...).</li> <li>1s—Repeating pattern of ones (...111...).</li> <li>2^15—Pseudo-random repeating pattern that is 32767 bits in length.</li> <li>2^20—Pseudo-random repeating pattern that is 1048575 bits in length.</li> <li>2^23—Pseudo-random repeating pattern that is 8388607 bits in length.</li> </ul>
<b>interval</b> <i>minutes</i>	Specifies the duration of the BERT test. The interval can be a value from 1 to 14400 minutes.

### Default

No BERT test is performed.

### Command Mode

Controller configuration

### Usage Guidelines

This command first appeared in Cisco IOS Release 11.3.

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** command. 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 to avoid 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 is to ensure consistency with telco numbering schemes for T1 channels within channelized T3 equipment.

---

### Example

In the following example, a BERT test pattern of all zeros is run for 30 minutes on T1 channel 6 on the CT3IP in slot 9:

```
controller t3 9/0/0
  t1 6 bert pattern 0s interval 30
```

## 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** controller configuration command.

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

### Syntax Description

<i>channel</i>	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.

### Default

Internal

### Command Mode

Controller configuration

### Usage Guidelines

This command first appeared in Cisco IOS Release 11.3.

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** 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 is to ensure consistency with telco numbering schemes for T1 channels within channelized T3 equipment.

---

### Example

In the following example, the clock source for T1 6 and T1 8 on the CT3IP are set to line:

```
controller t3 9/0/0
  t1 6 clock source line
  t1 8 clock source line
```

### Related Commands

You can use the master indexes or search online to find documentation of related commands.

**clock source**

## 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 the T1 channel can be further multiplexed on the Multichannel Interface Processor (MIP) or other multiplexing equipment, use the **t1 external** controller configuration command. Use the **no** form of this command to remove a T1 as an external port.

```
t1 external channel [cablelength feet] [linecode ami | b8zs]  
no t1 external channel
```

### Syntax Description

<i>channel</i>	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 0 to 655 feet. The default is 133 feet.
<b>linecode</b> <i>ami   b8zs</i>	(Optional) Specifies the line coding used by the T1. Values are alternate mark inversion (AMI) or bipolar 8 zero suppression (B8ZS). The default is B8ZS.

### Default

No external T1 is specified.

### Command Mode

Controller configuration

### Usage Guidelines

This command first appeared in Cisco IOS Release 11.3.

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 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 *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 controller 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 is to ensure 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.

---

### Example

In the following example, the T1 1 on the CT3IP is configured as an external port using AMI line coding and a cable length of 300 feet:

```
controller t3 9/0/0
  t1 external 1 cablelength 300 linecode ami
```

### Related Commands

You can use the master indexes or search online to find documentation of related commands.

**show controllers t3**



## 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** controller configuration command.

```
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 is used as the T1 framing type. This is the default.
<b>sf</b>	Specifies that super frame is used as the T1 framing type.

### Default

Extended super frame (ESF)

### Command Mode

Controller configuration

### Usage Guidelines

This command first appeared in Cisco IOS Release 11.3.

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 is to ensure consistency with telco numbering schemes for T1 channels within channelized T3 equipment.

---

### Example

In the following example, the framing for the T1 6 and T1 8 on the CT3IP are set to sf:

```
controller t3 9/0/0
  t1 6 framing sf
  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** controller configuration command.

```
t1 channel linecode {ami | b8zs}
```

### Syntax Description

<i>channel</i>	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.

### Default

B8ZS

### Command Mode

Controller configuration

### Usage Guidelines

This command first appeared in Cisco IOS Release 11.3.

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 is to ensure consistency with telco numbering schemes for T1 channels within channelized T3 equipment.

---

## Example

In the following example, the line coding for T1 channel 16 on the CT3IP is set to AMI:

```
controller t3 9/0/0
  t1 16 linecode ami
  exit
interface serial 9/0/0:16
  invert data
```

## Related Commands

You can use the master indexes or search online to find documentation of related commands.

**loopback remote (interface)**

## 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** controller configuration command. Use the **no** form of this command to remove the T1 channel from the test port.

```
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 from the T1 channel to the external CSU or MIP. Values are 0 to 655 feet. The default cable length is 133 feet.
<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). The default is B8ZS.

### Default

No test port is configured

### Command Mode

Controller configuration

### Usage Guidelines

This command first appeared in Cisco IOS Release 11.3.

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 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 controller 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 is to ensure 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.

---

### Example

In the following example, T1 6 on the CT3IP is configured as a test port using the default cable length and line coding:

```
controller t3 9/0/0
 t1 test 6
```

### Related Commands

You can use the master indexes or search online to find documentation of related commands.

**show controllers t3**

**t1 external**

## t1 timeslot

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

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

### Default

No timeslots are specified for the T1 channel.

### Command Mode

Controller configuration

### Usage Guidelines

This command first appeared in Cisco IOS Release 11.3.

You must specify the timeslots 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 is to ensure consistency with telco numbering schemes for T1 channels within channelized T3 equipment.

---

### Examples

In the following example, timeslots 1 through 24 are assigned to T1 1 for full T1 bandwidth usage:

```
controller t3 9/0/0  
t1 1 timeslots 1-24
```

In the following example, timeslots 1 to 5 and 20 to 23 are assigned to T1 6 for fractional T1 bandwidth usage:

```
controller t3 9/0/0  
t1 6 timeslots 1-5,20-23
```

In the following example, T1 8 is configured for  $n \times 56$  (where  $n$  is 24) bandwidth usage:

```
controller t3 9/0/0
 t1 8 timeslots 1-24 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** controller configuration command. Use the **no** form of this command to disable the detection and generation of yellow alarms.

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

### Syntax Description

<i>channel</i>	Number between 1 and 28 that indicates the T1 channel.
<b>detection</b>	Detect yellow alarms.
<b>generation</b>	Generate yellow alarms.

### Default

Yellow alarms are detected and generated on the T1 channel.

### Command Mode

Controller configuration

### Usage Guidelines

This command first appeared in Cisco IOS Release 11.3.

If the T1 framing type is superframe (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 is to ensure consistency with Telco numbering schemes for T1 channels within channelized T3 equipment.

---

### Example

In the following example, the yellow alarm detection is disabled on T1 channel 6 on the CT3IP:

```
controller t3 9/0/0  
  t1 6 framing sf  
  no t1 6 yellow detection
```

## test interface fastethernet

Use the **test interface fastethernet** EXEC command to test the Fast Ethernet interface by causing the interface to ping itself.

**test interface fastethernet** *number*

### Syntax Description

*number*

Port, connector, or interface card number. On a Cisco 4500 or Cisco 4700 series router, specifies the NPM 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.

### Command Mode

EXEC

### Usage Guidelines

This command first appeared in Cisco IOS Release 11.2.

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.

### Example

The following example tests a Fast Ethernet interface on a Cisco 4500:

```
test interface fastethernet 0
```

### Related Commands

You can use the master indexes or search online to find documentation of related commands.

**ping**

## 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, issue the **test service-module** privileged EXEC command.

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

### Syntax Description

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

### Command Mode

Privileged EXEC

### Usage Guidelines

This command first appeared in Cisco IOS Release 11.2.

A series of tests are performed on the CSU/DSU, which include a ROM checksum test, RAM test, EEPROM checksum test, flash checksum test, and a 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 five seconds when you issue this command. To view the output of the most recent self-tests, enable the **show service-module command**.

### Example

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

You can use the master indexes or search online to find documentation of related commands.

**clear counters**  
**clear service-module**  
**show service-module**

## timeslot

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

**timeslot** *start-slot* – *stop-slot*  
**no timeslot**

### Syntax Description

*start-slot*                      The first subframe in the major frame. Range is 1 to 31 and must be less than or equal to *stop-slot*.

*stop-slot*                        The last subframe in the major frame. Range is 1 to 31 and must be greater than or equal to *start-slot*.

### Default

A G.703 E1 interface is configured for unframed mode.

### Command Mode

Interface configuration

### Usage Guidelines

This command first appeared in Cisco IOS Release 10.3.

This command applies to a Cisco 4000 router or Cisco 7500 series router. 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.

### Example

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

```
timeslot 1-3
```

### Related Commands

You can use the master indexes or search online to find documentation of related commands.

**ts16**

## transmit-clock-internal

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

**transmit-clock-internal**  
**no transmit-clock-internal**

### Syntax Description

This command has no keywords or arguments.

### Default

Disabled

### Command Mode

Interface configuration

### Usage Guidelines

This command first appeared in Cisco IOS Release 10.0.

### Example

In the following example, the internally generated clock is enabled on serial interface 3/0 on a Cisco 7000 series or Cisco 7200 series router:

```
interface serial 3/0
 transmit-clock-internal
```

## transmitter-delay

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

```
transmitter-delay {delay}  
no transmitter-delay
```

### Syntax Description

*delay*            On the FSIP, HSSI, and on the IGS router, the minimum number of 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 131071.

### Default

0 flags or microseconds

### Command Mode

Interface configuration

### Usage Guidelines

This command first appeared in Cisco IOS Release 10.0.

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.

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 milliseconds 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.

### Example

The following example specifies a delay of 300 microseconds on serial interface 0:

```
interface serial 0  
  transmitter-delay 300
```

## ts16

To control the use of time slot 16 for data on a G.703 E1 interface, use the **ts16** interface configuration command. To restore the default, use the **no** form of this command.

```
ts16  
no ts16
```

### Syntax Description

This command has no arguments or keywords.

### Default

Time slot 16 is used for signaling.

### Command Mode

Interface configuration

### Usage Guidelines

This command first appeared in Cisco IOS Release 10.3.

This command applies to a Cisco 4000 router or Cisco 7500 series router. 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 timeslots, you must use the **ts16** command.

### Example

The following example configures time slot 16 to be used for data on a G.703 E1 interface:

```
ts16
```

### Related Commands

You can use the master indexes or search online to find documentation of related commands.

**timeslot**

## tunnel checksum

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

**tunnel checksum**  
**no tunnel checksum**

### Syntax Description

This command has no arguments or keywords.

### Default

Disabled

### Command Mode

Interface configuration

### Usage Guidelines

This command first appeared in Cisco IOS Release 10.0.

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.

### Example

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

```
tunnel checksum
```

## tunnel destination

To specify the destination for a tunnel interface, use the **tunnel destination** interface configuration command. 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

### Default

No tunnel interface destination is specified.

### Command Mode

Interface configuration

### Usage Guidelines

This command first appeared in Cisco IOS Release 10.0.

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.

### Examples

The following example enables Cayman tunneling:

```
interface tunnel0  
  tunnel source ethernet0  
  tunnel destination 131.108.164.19  
  tunnel mode cayman
```

The following example enables GRE tunneling:

```
interface tunnel0  
  appletalk cable-range 4160-4160 4160.19  
  appletalk zone Engineering  
  tunnel source ethernet0  
  tunnel destination 131.108.164.19  
  tunnel mode gre ip
```

### Related Commands

You can use the master indexes or search online to find documentation of related commands.

**appletalk cable-range**

**appletalk zone**

**tunnel mode**

**tunnel source**

## tunnel key

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

**tunnel key** *key-number*  
**no tunnel key**

### Syntax Description

*key-number*                      Number from 0 to 4294967295 that identifies the tunnel key.

### Default

Disabled

### Command Mode

Interface configuration

### Usage Guidelines

This command first appeared in Cisco IOS Release 10.0.

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

---

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

---

### Example

In the following example, the tunnel key is set to 3:

```
tunnel key 3
```

## tunnel mode

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

```
tunnel mode { aurp | cayman | dvmrp | eon | gre ip | nos }  
no tunnel mode
```

### Syntax Description

<b>aurp</b>	AppleTalk Update Routing Protocol (AURP).
<b>cayman</b>	Cayman TunnelTalk AppleTalk encapsulation.
<b>dvmrp</b>	Distance Vector Multicast Routing Protocol.
<b>eon</b>	EON compatible CLNS tunnel.
<b>gre ip</b>	Generic route encapsulation (GRE) protocol over IP.
<b>nos</b>	KA9Q/NOS compatible IP over IP.

### Default

GRE tunneling

### Command Mode

Interface configuration

### Usage Guidelines

This command first appeared in Cisco IOS Release 10.0. (The **aurp** and **dvmrp** options first appeared in Cisco IOS Release 10.3.)

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.

Cayman tunneling implements tunneling as designed by Cayman Systems. This enables our routers to interoperate with Cayman GatorBoxes. With Cayman tunneling, you can establish tunnels between two routers or between our router and a GatorBox. When using Cayman tunneling, you must not configure the tunnel with an AppleTalk network address. This means that there is no way to ping the other end of the tunnel.

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

Generic route encapsulation (GRE) tunneling can be done between our routers only. When using GRE tunneling for AppleTalk, you configure the tunnel with an AppleTalk network address. This means that you can ping the other end of the tunnel.

## Examples

The following example enables Cayman tunneling:

```
interface tunnel 0
 tunnel source ethernet 0
 tunnel destination 131.108.164.19
 tunnel mode cayman
```

The following example enables GRE tunneling:

```
interface tunnel 0
 appletalk cable-range 4160-4160 4160.19
 appletalk zone Engineering
 tunnel source ethernet0
 tunnel destination 131.108.164.19
 tunnel mode gre ip
```

## Related Commands

You can use the master indexes or search online to find documentation of related commands.

**appletalk cable-range**

**appletalk zone**

**tunnel destination**

**tunnel source**

## tunnel sequence-datagrams

To configure a tunnel interface to drop datagrams that arrive out of order, use the **tunnel sequence-datagrams** interface configuration command. 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.

### Default

Disabled

### Command Mode

Interface configuration

### Usage Guidelines

This command first appeared in Cisco IOS Release 10.0.

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).

### Example

In the following example, the tunnel is configured to drop datagrams that arrive out of order:

```
tunnel sequence-datagrams
```

## tunnel source

To set a tunnel interface's source address, use the **tunnel source** interface configuration command. 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 <b>show interfaces</b> command.

### Default

No tunnel interface's source address is set.

### Command Mode

Interface configuration

### Usage Guidelines

This command first appeared in Cisco IOS Release 10.0.

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** to an explicit IP address on the same subnet as the Cayman box, not the tunnel itself.

### Examples

The following example enables Cayman tunneling:

```
interface tunnel0  
tunnel source ethernet0  
tunnel destination 131.108.164.19  
tunnel mode cayman
```

The following example enables GRE tunneling:

```
interface tunnel0  
appletalk cable-range 4160-4160 4160.19  
appletalk zone Engineering  
tunnel source ethernet0  
tunnel destination 131.108.164.19  
tunnel mode gre ip
```

### Related Commands

You can use the index or search online to find documentation of related commands.

**appletalk cable-range**

**appletalk zone**

**tunnel destination**

## 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** interface configuration command.

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

### Syntax Description

*number* Maximum number of transmit buffers that the specified interface can subscribe.

### Default

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 Mode

Interface configuration

### Usage Guidelines

This command first appeared in Cisco IOS Release 10.0.

This command should be used only under the guidance of a technical support representative.

### Example

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

```
interface ethernet 0
tx-queue-limit 5
```

### Related Commands

You can use the master indexes or search online to find documentation of related commands.

**show controllers mci**