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 *ds1* **controller**

no t1 *ds1* **controller**

Syntax Description

ds1	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
controller	Configures a T1 and other types of controller and enters controller configuration mode.
controller t3	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** | **2^15** | **2^20** | **2^23**} **interval** *minutes*

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

Syntax Description

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

Defaults

No BERT test is performed.

Command Modes

Controller configuration

Command History

Release	Modification
11.3	This command was introduced.

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
show controllers t3	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.
internal	Specifies that the internal clock source is used. This is the default.
line	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
clock source (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

channel	Number 1, 2, or 3 that indicates the T1 channel.
cablelength *feet*	(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.
linecode ami | **b8zs**	(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
show controllers t3	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**

Syntax Description

channel	Number between 1 and 28 that indicates the T1 channel.

Defaults

Disabled

Command Modes

Controller configuration

Command History

Release	Modification
11.3	This command was introduced.

Usage Guidelines

The **t1 fdl ansi** command can be used only if the T1 framing type is Extended Super Frame (ESF).

To display the remote performance report information, use the **show controllers t3 remote performance** 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.

Examples

The following example shows how to generate the performance reports for T1 channel 8 on the CT3IP:

```
Router(config)# controller t3 9/0/0
Router(config-controller)# t1 8 fdl ansi
```

Related Commands

Command	Description
show controllers t3	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

channel	Number between 1 and 28 that indicates the T1 channel.
esf	Specifies that Extended Super Frame (ESF) is used as the T1 framing type. This is the default.
sf	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.
ami	Specifies that alternate mark inversion (AMI) line coding is used by the T1 channel.
b8zs	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
invert data	Inverts the data stream.
loopback remote (interface)	Loops packets through a CSU/DSU, over a DS3 link or a channelized T1 link, to the remote CSU/DSU and back.

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

channel	Number between 1 and 28 that indicates the T1 channel.
cablelength *feet*	(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.
linecode {**ami** | **b8zs**}	(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
show controllers t3	Displays the hardware and software driver information for a T3 controller.
t1 external	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

channel	Number between 1 and 28 that indicates the T1 channel.
range	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.
speed {**56** | **64**}	(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

channel	Number between 1 and 28 that indicates the T1 channel.
detection	Detects yellow alarms. This is the default, along with **generation**.
generation	Generates yellow alarms. This is the default, along with **detection**.

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 82 shows the questions asked of the user when the **test aim eeprom** command is entered, and the recommended user responses.

Table 82 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 **test aim eeprom** command dialog. The AIM slot number chosen is displayed, and the default command is the last command entered.

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

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

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

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

Examples

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

```
Router# test aim eeprom

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

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

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

test interface fastethernet

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

test interface fastethernet *number*

Syntax Description

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

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
11.2	This command was introduced.

Usage Guidelines

This command sends pings from the specified interface to itself. Unlike the **ping** command, the **test interface fastethernet** command does not require the use of an IP address.

Examples

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

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

Related Commands

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

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

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

timeslot

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

timeslot *start-slot stop-slot*

no timeslot

Syntax Description

start-slot	First subframe in the major frame. Valid range is from 1 to 31 and must be less than or equal to the *stop-slot* value.
stop-slot	Last subframe in the major frame. Valid range is from 1 to 31 and must be greater than or equal to the *start-slot* 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

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

transmit-buffers backing-store

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

transmit-buffers backing-store

no transmit-buffers backing-store

Syntax Description

This command has no arguments or keywords.

Defaults

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

Command Modes

Interface configuration

Command History

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

Usage Guidelines

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

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

Examples

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

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

Related Commands

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

transmit-clock-internal

To enable the internally generated clock on a serial interface on a Cisco 7200 series or Cisco 7500 series router when a DTE does not return a transmit clock, use the **transmit-clock-internal** command in interface configuration mode. To disable the 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

Syntax Description

delay	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.

Defaults

0 flags or microseconds

Command Modes

Interface configuration

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines

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 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.

Examples

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

tunnel checksum

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

tunnel checksum

no tunnel checksum

Syntax Description

This command has no arguments or keywords.

Defaults

Disabled

Command Modes

Interface configuration

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines

This command currently applies to generic 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 destination

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

tunnel destination {*host-name* | *ip-address*}

no tunnel destination

Syntax Description

host-name	Name of the host destination.
ip-address	IP address of the host destination expressed in dotted decimal notation.

Defaults

No tunnel interface destination is specified.

Command Modes

Interface configuration

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines

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

Examples

The following example shows how to configure the tunnel destination address for Cayman tunneling:

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

The following example shows how to configure the tunnel destination address for GRE (generic routing encapsulation) tunneling:

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

Related Commands

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

tunnel key

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

tunnel key *key-number*

no tunnel key

Syntax Description

key-number	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 multipoint** | **ipip** [**decapsulate-any**] | **iptalk** | **mpls** | **nos**}

no tunnel mode

Syntax Description

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

Defaults

GRE tunneling

Command Modes

Interface configuration

Command History

Release	Modification
10.0	This command was introduced.
10.3	The following keywords were added: • **aurp** • **dvmrp** • **ipip**
11.2	The optional **decapsulate-any** keyword was added.
12.2(13)T	The **gre multipoint** keyword was added.

Usage Guidelines

Source and Destination Address

You cannot have two tunnels that use the same encapsulation mode with exactly the same source and destination address. The work around 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 mrouted router to run DVMRP over a tunnel. You must configure Protocol Independent Multicast (PIM) and an IP address on a DVMRP tunnel.

GRE with AppleTalk

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

Multipoint GRE

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

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

Examples

Cayman Tunneling

The following example 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
```

Multipoint GRE Tunneling

The following example shows how to enable mGRE tunneling:

```
interface Tunnel0
```

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

Related Commands

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

tunnel path-mtu-discovery

To enable Path MTU Discovery (PMTUD) on a 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. • *aging-mins*—Number of minutes. Range is from 10 to 30. Default is 10. • **infinite**—Disables the age timer.
min-mtu	(Optional) Specifies the minimum Path MTU across GRE tunnels. • *mtu-bytes*—Number of bytes. Range is from 92 to 65535. Default is 92.

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 **min-mtu** keyword and *mtu-bytes* 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

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

tunnel sequence-datagrams

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

tunnel sequence-datagrams

no tunnel sequence-datagrams

Syntax Description

This command has no arguments or keywords.

Defaults

Disabled

Command Modes

Interface configuration

Command History

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 source

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

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

no tunnel source

Syntax Description

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

Defaults

No tunnel interface source address is set.

Command Modes

Interface configuration

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines

The source address is either an explicitly defined IP address or the IP address assigned to the specified interface.

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

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

Examples

The following example shows how to set a tunnel source address for Cayman tunneling:

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

The following example shows how to set a tunnel source address for GRE (generic routing encapsulation) tunneling:

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

Related Commands

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

tx-queue-limit

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

tx-queue-limit *number*

Syntax Description

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

Defaults

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

Command Modes

Interface configuration

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines

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

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

Examples

The following example shows how to set the maximum number of transmit buffers on the interface to 5:

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

Related Commands

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

yellow

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

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

Syntax Description

generation	Enables or disables generation of yellow alarms.
detection	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
```