

show ip interface

To display the usability status of interfaces configured for IP, use the **show ip interface** command in privileged EXEC mode.

show ip interface [*type number*] [**brief**]

Syntax Description	
<i>type</i>	(Optional) Interface type.
<i>number</i>	(Optional) Interface number.
brief	(Optional) Displays a summary of the usability status information for each interface.

Command Modes Privileged EXEC

Command History	Release	Modification
	10.0	This command was introduced.
	12.0(3)T	This command was expanded to include the status of ip wccp redirect out and ip wccp redirect exclude add in commands.
	12.2(14)S	This command was expanded to display the status of NetFlow on a subinterface.
	12.2(15)T	The command output enhancements introduced in Cisco IOS Release 12.2(14)S were integrated into Cisco IOS Release 12.2(15)T.
	12.3(6)	The command output was modified to identify the downstream VRF in the output.
	12.3(11)T	This command was integrated into Cisco IOS Release 12.3(11)T.
	12.3(14)YM2	This command was modified to show the usability status of interfaces configured for Multi-Processor Forwarding (MPF) and implemented on the Cisco 7301 and Cisco 7206VXR routers.
	12.4(4)T	This command was integrated into Cisco IOS Release 12.4(4)T.
	12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.

Usage Guidelines

The Cisco IOS software automatically enters a directly connected route in the routing table if the interface is usable. A usable interface can send and receive packets. If an interface is not usable, the directly connected routing entry is removed from the routing table. Removing the entry allows the software to use dynamic routing protocols to determine backup routes to the network, if any.

If the interface can provide two-way communication, the line protocol is marked “up.” If the interface hardware is usable, the interface is marked “up.”

If you specify an optional interface type, you see information for that specific interface.

If you specify no optional arguments, you see information on all the interfaces.

When an asynchronous interface is encapsulated with PPP or Serial Line Internet Protocol (SLIP), IP fast switching is enabled. A **show ip interface** command on an asynchronous interface encapsulated with PPP or SLIP displays a message indicating that IP fast switching is enabled.

The **show ip interface brief** command can be used to view a summary of the router interfaces. This command displays the IP address, interface status, and additional information.

Examples

The following examples from Cisco IOS Release 12.3(14)YM2 show:

- Configuration information on interface Gigabit Ethernet0/3, where the IP flow egress feature is configured on the output side (where packets go out of the interface) and the policy route-map named PBR_NAME is configured on the input side (where packets come into the interface).
- Interface information on Gigabit Ethernet interface 0/3 showing that MPF is enabled and that both features are not supported by MPF and are ignored.

The highlighted arrows (for documentation purposes only) show the configured output and input features and the additional MPF interface information.

```
Router# show running-config interface g 0/3
```

```
interface GigabitEthernet0/3
 ip address 10.1.1.1 255.255.0.0
 ip flow egress                <== output
 ip policy route-map PBR_NAME <== input
 duplex auto
 speed auto
 media-type gbic
 negotiation auto
end
```

```
Router# show ip interface g 0/3
```

```
GigabitEthernet0/3 is up, line protocol is up
 Internet address is 10.1.1.1/16
 Broadcast address is 255.255.255.255
 Address determined by setup command
 MTU is 1500 bytes
 Helper address is not set
 Directed broadcast forwarding is disabled
 Outgoing access list is not set
 Inbound access list is not set
 Proxy ARP is enabled
 Local Proxy ARP is disabled
 Security level is default
 Split horizon is enabled
 ICMP redirects are always sent
 ICMP unreachable are always sent
 ICMP mask replies are never sent
 IP fast switching is enabled
 IP fast switching on the same interface is disabled
 IP Flow switching is disabled
 IP CEF switching is enabled
 IP Feature Fast switching turbo vector
 IP VPN Flow CEF switching turbo vector
 IP multicast fast switching is enabled
 IP multicast distributed fast switching is disabled
 IP route-cache flags are Fast, CEF
 Router Discovery is disabled
 IP output packet accounting is disabled
 IP access violation accounting is disabled
 TCP/IP header compression is disabled
 RTP/IP header compression is disabled
 Policy routing is enabled, using route map PBR
 Network address translation is disabled
 BGP Policy Mapping is disabled
```

```

IP Multi-Processor Forwarding is enabled <===== MPF information
  IP Input features, "PBR",
    are not supported by MPF and are IGNORED
  IP Output features, "NetFlow",
    are not supported by MPF and are IGNORED

```

The following example identifies a downstream VRF. The highlighted line (for documentation purposes only) identifies the downstream VRF.

```
Router# show ip interface vi 3
```

```

Virtual-Access3 is up, line protocol is up
Interface is unnumbered. Using address of Loopback2 (10.0.0.8)
Broadcast address is 255.255.255.255
Peer address is 10.8.1.1
MTU is 1492 bytes
Helper address is not set
Directed broadcast forwarding is disabled
Outgoing access list is not set
Inbound access list is not set
Proxy ARP is enabled
Local Proxy ARP is disabled
Security level is default
Split horizon is enabled
ICMP redirects are always sent
ICMP unreachable are always sent
ICMP mask replies are never sent
IP fast switching is enabled
IP fast switching on the same interface is enabled
IP Flow switching is disabled
IP CEF switching is enabled
IP Feature Fast switching turbo vector
IP VPN CEF switching turbo vector
VPN Routing/Forwarding "U"
Downstream VPN Routing/Forwarding "D"
IP multicast fast switching is disabled
IP multicast distributed fast switching is disabled
IP route-cache flags are Fast, CEF
Router Discovery is disabled
IP output packet accounting is disabled
IP access violation accounting is disabled
TCP/IP header compression is disabled
RTP/IP header compression is disabled
Policy routing is disabled
Network address translation is disabled
WCCP Redirect outbound is disabled
WCCP Redirect inbound is disabled
WCCP Redirect exclude is disabled
BGP Policy Mapping is disabled

```

Table 53 describes the significant fields shown in the display.

Table 53 *show ip interface Field Descriptions*

Field	Description
Virtual-Access3 is up	If the interface hardware is usable, the interface is marked “up.” For an interface to be usable, both the interface hardware and line protocol must be up.
Broadcast address is	Displays the broadcast address.
Peer address is	Displays the peer address.
MTU is	Displays the MTU value set on the interface.
Helper address	Displays a helper address, if one has been set.
Directed broadcast forwarding	Indicates whether directed broadcast forwarding is enabled.
Outgoing access list	Indicates whether the interface has an outgoing access list set.
Inbound access list	Indicates whether the interface has an incoming access list set.
Proxy ARP	Indicates whether Proxy Address Resolution Protocol (ARP) is enabled for the interface.
Security level	Specifies the IP Security Option (IPSO) security level set for this interface.
Split horizon	Indicates that split horizon is enabled.
ICMP redirects	Specifies whether redirect messages will be sent on this interface.
ICMP unreachable	Specifies whether unreachable messages will be sent on this interface.
ICMP mask replies	Specifies whether mask replies will be sent on this interface.
IP fast switching	Specifies whether fast switching has been enabled for this interface. It is generally enabled on serial interfaces, such as this one.
IP Flow switching	Specifies whether Flow switching is enabled for this interface.
IP CEF switching	Specifies whether Cisco Express Forwarding is enabled for the interface.
Downstream VPN Routing/Forwarding “D”	Specifies the VRF where the PPP peer routes and AAA per-user routes are being installed.
IP multicast fast switching	Specifies whether multicast fast switching is enabled for the interface.
IP route-cache flags are Fast, Flow init, CEF, Ingress Flow	Specifies whether NetFlow has been enabled on an interface. Displays “Flow init” to specify that NetFlow is enabled on the interface. Displays “Ingress Flow” to specify that NetFlow is enabled on a subinterface using the ip flow ingress command. Specifies “Flow” to specify that NetFlow is enabled on a main interface using the ip route-cache flow command.

Table 53 *show ip interface Field Descriptions (continued)*

Field	Description
Router Discovery	Specifies whether the discovery process has been enabled for this interface. It is generally disabled on serial interfaces.
IP output packet accounting	Specifies whether IP accounting is enabled for this interface and what the threshold (maximum number of entries) is.
TCP/IP header compression	Indicates whether compression is enabled or disabled.
WCCP Redirect outbound is disabled	Indicates the status of whether packets received on an interface are redirected to a cache engine. Displays “enabled” or “disabled.”
WCCP Redirect exclude is disabled	Indicates the status of whether packets targeted for an interface will be excluded from being redirected to a cache engine. Displays “enabled” or “disabled.”

The following is sample output from the **show ip interface brief** command:

```
Router# show ip interface brief
```

```
Interface      IP-Address      OK?  Method  Status          Protocol
Ethernet0      10.108.00.5     YES  NVRAM   up              up
Ethernet1      unassigned      YES  unset   administratively down  down
Loopback0      10.108.200.5    YES  NVRAM   up              up
Serial0        10.108.100.5    YES  NVRAM   up              up
Serial1        10.108.40.5     YES  NVRAM   up              up
Serial2        10.108.100.5    YES  manual  up              up
Serial3        unassigned      YES  unset   administratively down  down
```

Table 54 *show ip interface brief Field Descriptions*

Field	Description
Interface	Type of interface.
IP-Address	IP Address assigned to the interface.
OK?	“Yes” means that the IP Address is currently valid. “No” means that the IP Address is not currently valid.

Table 54 *show ip interface brief Field Descriptions (continued)*

Field	Description
Method	<p>The method field has the following possible values:</p> <ul style="list-style-type: none"> • RARP or SLARP—Reverse Address Resolution Protocol (RARP) or Serial Line Address Resolution Protocol (SLARP) request • BOOTP—Bootstrap protocol • TFTP—Configuration file obtained from TFTP server • manual—Manually changed by CLI command • NVRAM—Configuration file in NVRAM • IPCP—ip address negotiated command • DHCP—ip address dhcp command • unassigned—No IP address • unset—Unset • other—Unknown
Status	<p>Indicates the status of interface. Valid values and their meanings are:</p> <ul style="list-style-type: none"> • up—Interface is administratively up. • down—Interface is administratively down. • administratively down—Interface is administratively down.
Protocol	<p>Indicates the operational status of the routing protocol on this interface.</p>

Related Commands

Command	Description
ip address	Sets a primary or secondary IP address for an interface.
ip vrf autoclassify	Enables VRF autoclassify on a source interface.
match ip source	Specifies a source IP address to match to required route maps that have been set up based on VRF connected routes.
route-map	Defines the conditions for redistributing routes from one routing protocol into another, or to enable policy routing.
set vrf	Enables VPN VRF selection within a route map for policy-based routing VRF selection.
show ip arp	Displays the ARP cache, in which SLIP addresses appear as permanent ARP table entries.
show route-map	Displays static and dynamic route maps.

show pas eswitch address

To display the Layer 2 learned addresses for an interface, use the **show pas eswitch address** EXEC command.

```
show pas eswitch address [ethernet | fastethernet] [slot/port]
```

Syntax Description	ethernet fastethernet	(Optional) Specify the type of interface.
	<i>slot</i>	(Optional) Slot number of the interface.
	<i>port</i>	(Optional) Interface number.

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

Command History	Release	Modification
	11.2 P	This command was introduced.

Examples

The following sample output shows that the first PA-12E/2FE interface (listed below as port 0) in port adapter slot 3 has learned the Layer 2 address 00e0.f7a4.5100 for bridge group 30 (listed below as BG 30):

```
Router# show pas eswitch address fastethernet 3/0
U 00e0.f7a4.5100, AgeTs 56273 s, BG 30 (vLAN 0), Port 0
```

show rif

To display the current contents of the RIF cache, use the **show rif** EXEC command.

show rif

Syntax Description This command has no arguments or keywords.

Command Modes EXEC

Release	Modification
10.0	This command was introduced.

Examples The following is sample output from the **show rif** command:

```
Router# show rif

Codes: * interface, - static, + remote
Hardware Addr How Idle (min) Routing Information Field
5C02.0001.4322 rg5 - 0630.0053.00B0
5A00.0000.2333 TR0 3 08B0.0101.2201.0FF0
5B01.0000.4444 - - -
0000.1403.4800 TR1 0 -
0000.2805.4C00 TR0 * -
0000.2807.4C00 TR1 * -
0000.28A8.4800 TR0 0 -
0077.2201.0001 rg5 10 0830.0052.2201.0FF0
```

In the display, entries marked with an asterisk (*) are the router/bridge's interface addresses. Entries marked with a dash (–) are static entries. Entries with a number are cached entries. If the RIF timeout is set to something other than the default of 15 minutes, the timeout is displayed at the top of the display.

Table 55 describes significant fields shown in the display.

Table 55 Show RIF Cache Display Field Descriptions

Field	Description
Hardware Addr	Lists the MAC-level addresses.
How	Describes how the RIF has been learned. Possible values include a ring group (rg), or interface (TR).
Idle (min)	Indicates how long, in minutes, since the last response was received directly from this node.
Routing Information Field	Lists the RIF.

show service-module serial

To display the performance report for an integrated CSU/DSU, use the **show service-module serial** privileged EXEC command.

```
show service-module serial number [performance-statistics [interval-range]]
```

Syntax Description		
	<i>number</i>	Interface number 0 or 1.
	performance-statistics	(Optional) Displays the CSU/DSU performance statistics for the past 24 hours. This keyword applies only to the fractional T1/T1 module.
	<i>interval-range</i>	(Optional) Specifies the number of 15-minute intervals displayed. You can choose a range from 1 to 96, where each value represents the CSU/DSU activity performed in that 15-minute interval. For example, a range of 2-3 displays the performance statistics for the intervals two and three.

Command Modes	
	Privileged EXEC

Command History	Release	Modification
	11.2	This command was introduced.

Usage Guidelines	
	This command applies to the 2- and 4-wire 56/64-kbps CSU/DSU module and FT1/T1 CSU/DSU module. The performance-statistics keyword applies only to the FT1/T1 CSU/DSU module.

Examples

The following sample output shows CSU/DSU performance statistics on a Cisco 2524 or Cisco 2525 router for intervals 30 to 32. Each interval is 15 minutes long. All the data is zero because no errors were discovered on the T1 line:

```
Router# show service-module serial 1 performance-statistics 30-32

Total Data (last 58 15 minute intervals):
  0 Line Code Violations, 0 Path Code Violations
  0 Slip Secs, 0 Fr Loss Secs, 0 Line Err Secs, 0 Degraded Mins
  0 Errored Secs, 0 Bursty Err Secs, 0 Severely Err Secs, 0 Unavail Secs
Data in current interval (131 seconds elapsed):
  0 Line Code Violations, 0 Path Code Violations
  0 Slip Secs, 0 Fr Loss Secs, 0 Line Err Secs, 0 Degraded Mins
  0 Errored Secs, 0 Bursty Err Secs, 0 Severely Err Secs, 0 Unavail Secs
Data in Interval 30:
  0 Line Code Violations, 0 Path Code Violations
  0 Slip Secs, 0 Fr Loss Secs, 0 Line Err Secs, 0 Degraded Mins
  0 Errored Secs, 0 Bursty Err Secs, 0 Severely Err Secs, 0 Unavail Secs
Data in Interval 31:
  0 Line Code Violations, 0 Path Code Violations
  0 Slip Secs, 0 Fr Loss Secs, 0 Line Err Secs, 0 Degraded Mins
  0 Errored Secs, 0 Bursty Err Secs, 0 Severely Err Secs, 0 Unavail Secs
Data in Interval 32:
  0 Line Code Violations, 0 Path Code Violations
  0 Slip Secs, 0 Fr Loss Secs, 0 Line Err Secs, 0 Degraded Mins
  0 Errored Secs, 0 Bursty Err Secs, 0 Severely Err Secs, 0 Unavail Secs
```

The following example is sample output from the **show service-module serial** command:

```
Router1# show service-module serial 0

Module type is T1/fractional
  Hardware revision is B, Software revision is 1.1 ,
  Image checksum is 0x2160B7C, Protocol revision is 1.1
Receiver has AIS alarm,
Unit is currently in test mode:
  line loopback is in progress
Framing is ESF, Line Code is B8ZS, Current clock source is line,
Fraction has 24 timeslots (64 Kbits/sec each), Net bandwidth is 1536 Kbits/sec.
Last user loopback performed:
  remote loopback
  Failed to loopup remote
Last module self-test (done at startup): Passed
Last clearing of alarm counters 0:05:50
  loss of signal      :    1, last occurred 0:01:50
  loss of frame       :    0,
  AIS alarm           :    1, current duration 0:00:49
  Remote alarm        :    0,
  Module access errors :    0,
Total Data (last 0 15 minute intervals):
Line Code Violations, 0 Path Code Violations
  0 Slip Secs, 0 Fr Loss Secs, 0 Line Err Secs, 0 Degraded Mins
  0 Errored Secs, 0 Bursty Err Secs, 0 Severely Err Secs, 0 Unavail Secs
Data in current interval (351 seconds elapsed):
  1466 Line Code Violations, 0 Path Code Violations
  25 Slip Secs, 49 Fr Loss Secs, 40 Line Err Secs, 1 Degraded Mins
  0 Errored Secs, 0 Bursty Err Secs, 0 Severely Err Secs, 49 Unavail Secs

Router1# show service-module serial 1

Module type is 4-wire Switched 56
  Hardware revision is B, Software revision is 1.00,
  Image checksum is 0x44453634, Protocol revision is 1.0
Connection state: active,
Receiver has loss of signal, loss of sealing current,
Unit is currently in test mode:
  line loopback is in progress
Current line rate is 56 Kbits/sec
Last user loopback performed:
  dte loopback
  duration 00:00:58
Last module self-test (done at startup): Passed
Last clearing of alarm counters 0:13:54
  oos/oof             :    3, last occurred 0:00:24
  loss of signal      :    3, current duration 0:00:24
  loss of sealing curren:    2, current duration 0:04:39
  loss of frame       :    0,
  rate adaption attempts:    0,
```

The following example shows sample output from the **show service-module serial** command issued on a Cisco 3640 modular access router:

```
router# show service-module serial 0/1

Module type is 4-wire Switched 56
  Hardware revision is B, Software revision is 1.00,
  Image checksum is 0x42364436, Protocol revision is 1.0
Connection state: Idle
Receiver has no alarms.
CSU/DSU Alarm mask is 0
Current line rate is 56 Kbits/sec
Last module self-test (done at startup): Passed
Last clearing of alarm counters 4d02h
  oos/oof           : 0,
  loss of signal    : 0,
  loss of sealing curren: 0,
  loss of frame     : 0,
  rate adaptation attemp: 0,
```

The following example shows sample output from the **show service-module serial** command issued on a Cisco 1605 router:

```
router# show service-module serial 0

Module type is 4-wire Switched 56
  Hardware revision is B, Software revision is 1.00,
  Image checksum is 0x42364436, Protocol revision is 1.0
Receiver has oos/oof, loss of signal,
CSU/DSU Alarm mask is 4
Current line rate is 56 Kbits/sec
Last module self-test (done at startup): Passed
Last clearing of alarm counters 1d02h
  oos/oof           : 1, current duration 1d02h
  loss of signal    : 1, current duration 1d02h
  loss of frame     : 0,
  rate adaptation attemp: 0,
```

Table 56 describes the fields displayed by the **show service-module serial** command.

Table 56 *show service-module Output Field Descriptions*

Field	Description
Module type	The CSU/DSU module installed in the router. The possible modules are T1/fractional, 2-wire switched 56-kbps, and 4-wire 56/64-kbps.
Receiver has AIS alarm	Alarms detected by the FT1/T1 CSU/DSU module or 2- and 4-wire 56/64-kbps CSU/DSU modules. Possible T1 alarms are as follows: <ul style="list-style-type: none"> • Transmitter is sending remote alarm. • Transmitter is sending AIS. • Receiver has loss of signal. • Receiver has loss of frame. • Receiver has remote alarm. • Receiver has no alarms. Possible switched 56k alarms are as follows: <ul style="list-style-type: none"> • Receiver has loss of signal • Receiver has loss of sealing current • Receiver has loss of frame • Receiver has rate adaptation attempts
Unit is currently in test mode	Loopback tests are in progress.
Framing is ESF	Indicates frame type used on the line. Can be extended super frame or super frame.
Line Code is B8ZS	Indicated line-code type configured. Can be alternate mark inversion (AMI) or binary 8-zero substitution (B8ZS).
Current clock source is line	Clock source configured on the line, which can be supplied by the service provider (line) or the integrated CSU/DSU module (internal).
Fraction has 24 timeslots	Number of timeslots defined for the FT1/T1 module, which can range from 1 to 24.
Net bandwidth	Total bandwidth of the line (for example, 24 timeslots multiplied by 64 kbps equals a bandwidth of 1536 kbps).
Last user loopback performed	Type and outcome of the last performed loopback.
Last module self-test (done at startup): Passed	Status of the last self test performed on an integrated CSU/DSU module.
Last clearing of alarm counters	List of network alarms that were detected and cleared on the CSU/DSU module.
Total Data Data in current interval	Shows the current accumulation period, which rolls into the 24-hour accumulation every 15 minutes. The oldest 15-minute period falls off the back of the 24-hour accumulation buffer.
Line Code Violations	Indicates the occurrence of either a bipolar violation or excessive zeroes error event.

Table 56 *show service-module Output Field Descriptions (continued)*

Field	Description
Path Code Violations	Indicates a frame synchronization bit error in the D4 and E1-no CRC formats or a CRC error in the ESF and E1-CRC formats.
Slip Secs	Indicates the replication or detection of the payload bits of a DS1 frame. A slip may be performed when there is a difference between the timing of a synchronous receiving terminal and the received signal.
Fr Loss Secs	Indicates the number of seconds an out of frame error is detected.
Line Err Secs	Line errored seconds is a second in which one or more line code violation errors are detected.
Errored Secs	In ESF and E1-CRC links, an errored second is a second in which one of the following is detected: one or more path code violations; one or more out of frame defects; one or more controlled slip events; a detected AIS defect. For D4 and E1-no CRC links, the presence of bipolar violation also triggers an errored second.
Bursty Err Secs	A second with fewer than 320 and more than 1 path coding violation errors. No severely errored frame defects or incoming AIS defects are detected. Controlled slips are not included in this parameter.
Severely Err Secs	For ESF signals, a second with one of the following errors: 320 or more path code violation errors; one or more out of frame defects; a detected AIS defect. For D4 signals, a count of 1-second intervals with framing errors, or an out of frame defect, or 1544 line code violations.
Unavail Secs	Total time the line was out of service.

Related Commands

Command	Description
clear service-module serial	Resets an integrated CSU/DSU.

show smf

To display the configured software MAC address filter (SMF) on various interfaces of a router, use the **show smf EXEC** command.

```
show smf [interface-name]
```

Syntax Description	<i>interface-name</i>	Displays information about the specified interface. Choices can include atm, ethernet, fastethernet, null, serial, tokenring, and async.
---------------------------	-----------------------	--

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

Command History	Release	Modification
	10.0	This command was introduced in a release prior to 10.0.

Usage Guidelines The SMF is active whenever the router is doing bridging or IRB. MAC address filtering can be used as a security feature in bridging or switching environments.

Examples The following is sample output from the **show smf** command:

```
R2-81-7206#sh smf

Software MAC address filter on FastEthernet0/0.2
Hash Len   Address           Matches  Act      Type
0x00:  0  ffff.ffff.ffff      0  RCV  Physical broadcast
0x0C:  0  0100.0c00.0000      0  RCV  ISL vLAN Multicast
0x2A:  0  0900.2b01.0001      0  RCV  DEC spanning tree
0xA6:  0  0010.a6ae.6000      0  RCV  Interface MAC address
0xC1:  0  0100.0ccc.cccd      0  RCV  SSTP MAC address
0xC2:  0  0180.c200.0000      0  RCV  IEEE spanning tree
0xC2:  1  0180.c200.0000      0  RCV  IBM spanning tree
0xC2:  2  0100.0ccd.cdce      0  RCV  VLAN Bridge STP
```

N

Table 57 describes the fields shown in this display.

Table 57 *show smf* Field Descriptions

Field	Description
Hash	Position in the hash table for this entry.
Len	Length of the entry.
Address	MAC address for the interface.
Matches	Number of hits for the address

Table 57 show smf Field Descriptions (continued)

Field	Description
Act	Action taken. Values can be receive (RCV), forward (FWD), or discard (DIS).
Type	Type of MAC address.

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.

Defaults Enabled

Command Modes Controller configuration

Command History	Release	Modification
	11.3	This command was introduced.

Usage Guidelines 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.

Examples The following example shuts down the CT3IP:

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

Related Commands	Command	Description
	show controllers t3	Displays information about the CT3IP on Cisco 7500 series routers.

shutdown (hub)

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 Modes Hub configuration

Command History	Release	Modification
	10.3	This command was introduced.

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

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

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

shutdown (interface)

To disable an interface, use the **shutdown** 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.

Defaults Enabled

Command Modes Interface configuration

Command History	Release	Modification
	10.0	This command was introduced.

Usage Guidelines 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	Command	Description
	interface	Configures an interface type and enters interface configuration mode.
	show interfaces	Displays statistics for all interfaces configured on the router or access server.

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	<i>number</i>	Number of buffers used to store unprocessed SMT messages that are to be queued for processing. Acceptable values are positive integers.
---------------------------	---------------	---

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

Command Modes	Global configuration
----------------------	----------------------

Command History	Release	Modification
	10.0	This command was introduced.

Usage Guidelines	This command helps ensure that the routers keep track of FDDI <i>upstream</i> and <i>downstream</i> 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.
-------------	--

Examples	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.

Defaults No SNMP trap is issued.

Command Modes Hub configuration

Command History	Release	Modification
	11.1	This command was introduced.

Usage Guidelines 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).

Examples 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

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

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	<i>mac-address</i> (Optional) MAC address in the packets that the hub will allow to access the network.				
Defaults	Disabled				
Command Modes	Hub configuration				
Command History	<table border="1"> <thead> <tr> <th style="border-top: 1px solid black; border-bottom: 1px solid black;">Release</th> <th style="border-top: 1px solid black; border-bottom: 1px solid black;">Modification</th> </tr> </thead> <tbody> <tr> <td style="border-bottom: 1px solid black;">10.3</td> <td style="border-bottom: 1px solid black;">This command was introduced.</td> </tr> </tbody> </table>	Release	Modification	10.3	This command was introduced.
Release	Modification				
10.3	This command was introduced.				
Usage Guidelines	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	<p>The following example configures the hub to allow only packets from MAC address 1111.2222.3333 on port 2 of hub 0:</p> <pre>hub ethernet 0 2 source-address 1111.2222.3333</pre> <p>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:</p> <pre>hub ethernet 0 2 source-address</pre>				
Related Commands	<table border="1"> <thead> <tr> <th style="border-top: 1px solid black; border-bottom: 1px solid black;">Command</th> <th style="border-top: 1px solid black; border-bottom: 1px solid black;">Description</th> </tr> </thead> <tbody> <tr> <td style="border-bottom: 1px solid black;">hub</td> <td style="border-bottom: 1px solid black;">Enables and configures a port on an Ethernet hub of a Cisco 2505 or Cisco 2507.</td> </tr> </tbody> </table>	Command	Description	hub	Enables and configures a port on an Ethernet hub of a Cisco 2505 or Cisco 2507.
Command	Description				
hub	Enables and configures a port on an Ethernet hub of a Cisco 2505 or Cisco 2507.				

speed

To configure the speed for a Fast Ethernet interface, use the **speed** interface configuration command. Use the **no** form of this command to disable a speed setting.

speed { **10** | **100** | **auto** }

no speed

Syntax Description	
10	Configures the interface to transmit at 10 Mbps.
100	Configures the interface to transmit at 100 Mbps.
auto	Turns on the Fast Ethernet auto-negotiation capability. The interface automatically operates at 10 or 100 Mbps depending on environmental factors, such as the type of media and transmission speeds for the peer routers, hubs, and switches used in the network configuration.

Defaults 100 Mbps

Command Modes Interface configuration

Command History	Release	Modification
	11.2(10)P	This command was introduced.

Usage Guidelines The auto negotiation capability is turned on for the Fast Ethernet interface by either configuring the **speed auto** interface configuration command or the **duplex auto** interface configuration command. Table 58 describes the system's performance for different combinations of the duplex and speed modes. The specified **duplex** command configured with the specified **speed** command produces the resulting system action.

Table 58 Relationship between Duplex and Speed Commands

Duplex Command	Speed Command	Resulting System Action
duplex auto	speed auto	Auto negotiates both speed and duplex modes.
duplex auto	speed 100 or speed 10	Auto negotiates both speed and duplex modes.
duplex half or duplex full	speed auto	Auto negotiates both speed and duplex modes.
duplex half	speed 10	Forces 10 Mbps and half duplex.
duplex full	speed 10	Forces 10 Mbps and full duplex.

Table 58 Relationship between Duplex and Speed Commands (continued)

Duplex Command	Speed Command	Resulting System Action
duplex half	speed 100	Forces 100 Mbps and half duplex.
duplex full	speed 100	Forces 100 Mbps and full duplex.

Examples

The following example shows the configuration options for the **speed** command:

```
router# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
router(config)# interface fastethernet 0
router(config-if)# speed ?
  10    Force 10 Mbps operation
  100   Force 100 Mbps operation
  auto  Enable AUTO speed configuration
```

Related Commands

Command	Description
duplex	Configures the duplex operation on an interface.
interface fastethernet	Selects a particular Fast Ethernet interface for configuration.
show controllers fastethernet	Displays information about initialization block information, transmit ring, receive ring, and errors for the Fast Ethernet controller chip on the Cisco 4500, Cisco 7200 series, or Cisco 7500 series routers.
show interfaces fastethernet	Displays information about the FastEthernet interfaces.

squelch

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

```
squelch {normal | reduced}
```

```
no squelch {normal | reduced}
```

Syntax Description

normal	Allows normal capability.
reduced	Allows extended 10BaseT capability.

Defaults

Normal range

Command Modes

Interface configuration

Command History

Release	Modification
10.0	This command was introduced.

Examples

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

```
interface ethernet 2
  squelch 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.
pattern		Specifies the length of the repeating BERT test pattern. Values are:
0s		0s—Repeating pattern of zeros (...000...).
1s		1s—Repeating pattern of ones (...111...).
2^15		2^15—Pseudo-random repeating pattern that is 32767 bits in length.
2^20		2^20—Pseudo-random repeating pattern that is 1048575 bits in length.
2^23		2^23—Pseudo-random repeating pattern that is 8388607 bits in length.
interval <i>minutes</i>		Specifies the duration of the BERT test. The interval can be a value from 1 to 14400 minutes.

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** 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.

Examples

The following example runs a BERT test pattern of all zeros 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	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 is to ensure consistency with telco numbering schemes for T1 channels within channelized T3 equipment.

Examples The following example sets the clock source for T1 6 and T1 8 on the CT3IP to line:

```
controller t3 9/0/0
 t1 6 clock source line
 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 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.
cablelength <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.
linecode <i>ami</i> b8zs	(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.

Defaults No external T1 is specified.

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 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.

Examples

The following example configures the T1 1 on the CT3IP 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


Command	Description
show controllers t3	Displays information about the CT3IP on Cisco 7500 series routers.

t1 fdl ansi

To enable the one-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** controller configuration command. Use the **no** form of this command to disable the performance report.

t1 channel fdl ansi

no t1 channel fdl ansi

Syntax Description	<i>channel</i> Number between 1 and 28 that indicates the T1 channel.				
Defaults	Disabled				
Command Modes	Controller configuration				
Command History	<table border="1"> <thead> <tr> <th>Release</th> <th>Modification</th> </tr> </thead> <tbody> <tr> <td>11.3</td> <td>This command was introduced.</td> </tr> </tbody> </table>	Release	Modification	11.3	This command was introduced.
Release	Modification				
11.3	This command was introduced.				
Usage Guidelines	<p>The t1 fdl ansi command can be used only if the T1 framing type is extended superframe (ESF). To display the remote performance report information, use the show controllers t3 remote performance command.</p>				
 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	<p>The following example generates the performance reports for T1 channel 8 on the CT3IP:</p> <pre>controller t3 9/0/0 t1 8 fdl ansi</pre>				
Related Commands	<table border="1"> <thead> <tr> <th>Command</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td>show controllers t3</td> <td>Displays information about the CT3IP on Cisco 7500 series routers.</td> </tr> </tbody> </table>	Command	Description	show controllers t3	Displays information about the CT3IP on Cisco 7500 series routers.
Command	Description				
show controllers t3	Displays information about the CT3IP on Cisco 7500 series routers.				

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	channel	Number between 1 and 28 that indicates the T1 channel.
	esf	Specifies that extended super frame is used as the T1 framing type. This is the default.
	sf	Specifies that super frame 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 is to ensure consistency with telco numbering schemes for T1 channels within channelized T3 equipment.

Examples The following example sets the framing for the T1 6 and T1 8 on the CT3IP 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.
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.

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

Examples

The following example sets the line coding for T1 channel 16 on the CT3IP to AMI:

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

Related Commands

Command	Description
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** 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.
<i>cablelength</i> <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.
<i>linecode</i> { 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). The default is B8ZS.

Defaults	
	No test port is configured

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 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.

Examples

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

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

Related Commands

Command	Description
show controllers t3	Displays information about the CT3IP on Cisco 7500 series routers.
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 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.
timeslot range	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.
speed {56 64}	(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.

Defaults No timeslots are specified for the T1 channel.

Command Modes Controller configuration

Command History	Release	Modification
	11.3	This command was introduced.

Usage Guidelines 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 The following example assigns timeslots 1 through 24 to T1 1 for full T1 bandwidth usage:

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

The following example assigns timeslots 1 to 5 and 20 to 23 to T1 6 for fractional T1 bandwidth usage:

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

The following example configures T1 8 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 t1 channel yellow {detection | generation}
```

Syntax Description

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

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 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.

Examples

The following example disables the yellow alarm detection 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	<i>number</i>	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 Modes	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 tests a Fast Ethernet interface on a Cisco 4500:

```
test interface fastethernet 0
```

Related Commands	Command	Description
	ping (privileged)	Diagnoses basic network connectivity on Apollo, AppleTalk, Connectionless Network Service (CLNS), DECnet, IP, Novell IPX, VINES, or XNS networks.
	ping (user)	Diagnoses basic network connectivity on AppleTalk, CLNS, IP, Novell, Apollo, VINES, DECnet, or XNS networks.

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 Modes

Privileged EXEC

Command History

Release	Modification
11.2	This command was introduced.

Usage Guidelines

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.

Examples

This example performs a self test on serial interface 0:

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

Related Commands

Command	Description
clear counters	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 serial interface on a G.703 E1 port adapter, an FSIP, or an E1-G.703/G.704 serial port adapter, 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		
<i>start-slot</i>	The first subframe in the major frame. Range is 1 to 31 and must be less than or equal to <i>stop-slot</i> .	
<i>stop-slot</i>	The last subframe in the major frame. Range is 1 to 31 and must be greater than or equal to <i>start-slot</i> .	

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

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

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

```
interface serial 3/0
 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** interface configuration command. To disable this function, use the **no** form of this command.

transmit-buffers backing-store

no transmit-buffers backing-store

Syntax Description

This command has no arguments or keywords.

Defaults

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

Command Modes

Interface configuration

Command History

Release	Modification
10.3	This command was introduced on the Cisco 7500 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

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 arguments or keywords.

Defaults Disabled

Command Modes Interface configuration

Release	Modification
10.0	This command was introduced.

Examples The following example enables the internally generated clock on serial interface 3/0 on a Cisco 7000 series or Cisco 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. Use the **no** form of this command restores the default.

transmitter-delay *delay*

no transmitter-delay

Syntax Description	<i>delay</i>	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.
---------------------------	--------------	--

Defaults	0 flags or microseconds
-----------------	-------------------------

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

Command History	Release	Modification
	10.0	This command was introduced.

Usage Guidelines	<p>This command is especially useful for serial interfaces that can send back-to-back data packets over serial interfaces faster than some hosts can receive them.</p> <p>The transmitter delay feature is implemented for the following Token Ring cards: CSC-R16, CSC-R16M, CSC-1R, CSC-2R, and CSC-CTR. For the first four cards, the command syntax is the same as the existing command and specifies the number of 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.</p>
-------------------------	--

Examples	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 or on a E1-G703/G.704 serial port adapter, 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.

Defaults Time slot 16 is used for signaling.

Command Modes Interface configuration

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

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

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

```
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** 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.

Defaults Disabled

Command Modes Interface configuration

Release	Modification
10.0	This command was introduced.

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

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

```
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

Defaults No tunnel interface destination is specified.

Command Modes Interface configuration

Command History	Release	Modification
	10.0	This command was introduced.

Usage Guidelines You cannot have two tunnels using the same encapsulation mode with exactly the same source and destination address. The workaround is to create a loopback interface and source packets off of the loopback interface. Refer to *Network Protocols, Part 2* for more information on AppleTalk Cayman tunneling.

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

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** interface configuration command. To remove the ID key, use the **no** form of this command.

tunnel key *key-number*

no tunnel key

Syntax Description	<i>key-number</i>	Number from 0 to 4294967295 that identifies the tunnel key.
--------------------	-------------------	---

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

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

Command History	Release	Modification
	10.0	This command was introduced.

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



Note

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



Note

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

Examples The following example sets the tunnel key to 3:

```
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 | ipip [decapsulate-any] | iptalk | mpls | nos }
no tunnel mode
```

Syntax Description	
aurp	AppleTalk Update Routing Protocol (AURP).
cayman	Cayman TunnelTalk AppleTalk encapsulation.
dvmrp	Distance Vector Multicast Routing Protocol.
eon	EON compatible CLNS tunnel.
gre	Generic route encapsulation (GRE) protocol. This is the default.
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	MPLS encapsulation.
nos	KA9Q/NOS compatible IP over IP.

Defaults GRE tunneling

Command Modes Interface configuration

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

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

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 mouted router 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

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 source	Sets the source address of a tunnel interface.

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.

Defaults Disabled

Command Modes Interface configuration

Release	Modification
10.0	This command was introduced.

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

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

```
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 show interfaces command.

Defaults No tunnel interface's source address is set.

Command Modes Interface configuration

Command History	Release	Modification
	10.0	This command was introduced.

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

When using tunnels to Cayman boxes, you must set the **tunnel source** 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

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

tx-queue-limit

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

tx-queue-limit *number*

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

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

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

Command History	Release	Modification
	10.0	This command was introduced.

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

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

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

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