Overview of Interface Configuration

Use the information in this chapter to understand the types of interfaces supported on Cisco routers and access servers and to locate configuration information for various types of interfaces.

For a complete description of the interface commands used in this and other chapters that describe interface configuration, refer to the "Interface Commands" chapter of the *Configuration Fundamentals Command Reference*. To locate documentation of other commands that appear in this chapter, use the command reference master index or search online.

This chapter contains general information that applies to all interface types; it includes these sections:

- Interface Types Supported on Cisco Routers
- Understand Interface Configuration
- Understand Subinterfaces
- Configure Features Available on any Interface
- Understand Online Insertion and Removal (OIR)
- Understand Fast Switching Support
- Monitor and Maintain the Interface

For examples of configuration tasks shown in this chapter, see "Interface Configuration Examples" at the end of this chapter.

For information about a specific type of interface, refer to the chapter or publication indicated here:

For this interface type . . .	And these tasks . . .	See this chapter or publication . . .
Dialed interfaces	• Configure Channelized E1, Channelized T1, or Channelized T1 on the Cisco AS5200 • Configure a Dialer Interface • Configure an ISDN BRI, MBRI, or PRI Interface	*Dial Solutions Configuration Guide* and *Dial Solutions Command Reference*

For this interface type . . .	And these tasks . . .	See this chapter or publication . . .
LAN interfaces	• Configure an Ethernet or Fast Ethernet Interface • Configure a Fiber Distributed Data Interface (FDDI) • Configure a Hub Interface • Configure a LAN Extender Interface • Configure a Token Ring Interface	"Configuring LAN Interfaces" chapter in this publication
Serial interfaces	• Configure a High-Speed Serial Interface (HSSI) • Configure a Synchronous Serial Interface • Configure a Packet OC-3 Interface • Configure Serial Interfaces for CSU/DSU Service Modules • Configure Low-Speed Serial Interfaces	"Configuring Serial Interfaces" chapter in this publication
Logical or virtual interfaces	• Configure a Loopback Interface • Configure a Null Interface • Configure a Tunnel Interface	"Configuring Logical Interfaces" chapter in this publication
Channel Interface Processor (CIP)	Configure a Channel Interface Processor	"Configuring IBM Channel Attach" in the *Bridging and IBM Networking Configuration Guide*.

Note In Cisco IOS Release 11.3, all commands supported on the Cisco 7500 series are also supported on the Cisco 7000 series.

Interface Types Supported on Cisco Routers

Two types of interfaces are supported: physical and virtual interfaces. The types of physical interfaces on a device depend on its interface processors or port adapters. The virtual interfaces that Cisco routers and access servers support include subinterfaces and IP tunnels.

Cisco routers and access servers support the following types of interfaces:

- Asynchronous serial
- Asynchronous Transfer Mode (ATM)
- Channelized E1
- Channelized T1
- Dialer
- Ethernet
- Fast Ethernet
- Fiber Distributed Data Interface (FDDI)
- Fractional T1/T1

- High-Speed Serial Interface (HSSI)
- ISDN Basic Rate Interface (BRI)
- ISDN Multiple Basic Rate Interface (MBRI)
- ISDN Primary Rate Interface (PRI)
- LAN Extender
- Loopback
- Low-Speed Serial
- Null
- Packet OC-3
- Synchronous serial
- Token Ring
- Tunnel

In addition, the Cisco IOS software supports subinterfaces. See the *Wide-Area Networking Configuration Guide* and the protocol chapters in the Cisco IOS software configuration guides for specific information on how to configure a subinterface for a particular protocol.

For hardware technical descriptions and information about installing interfaces, refer to the hardware installation and maintenance publication for your product. For command descriptions and usage information, refer to the "Interface Commands" chapter of the *Configuration Fundamentals Command Reference*.

Understand Interface Configuration

These general instructions apply to all interface configuration processes. Begin interface configuration in global configuration mode. To configure an interface, follow these steps:

Step 1 Enter the **configure** EXEC command at the privileged EXEC prompt to enter global configuration mode.

Step 2 Once in the global configuration mode, start configuring the interface by entering the **interface** command. Identify the interface type followed by the number of the connector or interface card. These numbers are assigned at the factory at the time of installation or when cards are added to a system and can be displayed with the **show interfaces** EXEC command. A report is provided for each interface that the device supports, as seen in the following partial sample display:

```
Router# show interfaces
Serial 0 is administratively down, line protocol is down
Hardware is MCI Serial
MTU 1500 bytes, BW 1544 Kbit, DLY 20000 usec, rely 255/255, load 1/255
Encapsulation HDLC, loopback not set, keepalive set (10 sec)
```

Use the **show hardware** EXEC command to see a list of the system software and hardware.

To begin configuring serial interface 0, you add the following line to the configuration file:

```
interface serial 0
```

Note It is not necessary to add a space between the interface type and interface number. For example, in the preceding line you can specify either *serial 0* or *serial0*. The command will work either way.

Step 3 Follow each **interface** command with the interface configuration commands your particular interface requires. The commands you enter define the protocols and applications that will run on the interface. The commands are collected and applied to the **interface** command until you enter another **interface** command, a command that is not an interface configuration command, or you type the Ctrl-Z sequence to get out of configuration mode and return to privileged EXEC mode.

Step 4 Once an interface is configured, you can check its status by entering the EXEC **show** commands described after the task tables that follow.

Note Configuring channelized T1 and E1 interfaces requires additional steps. When you configure channelized T1or channelized E1, you must first define the channels and the time slots that comprise the channels by using the **controller t1** and the **channel-group** controller configuration commands. Then configure the virtual serial interfaces using the **interface serial** global configuration commands. Refer to the Cisco IOS *Dial Solutions Configuration Guide* for instructions on configuring channelized E1 or channelized T1 interfaces.

Understand Subinterfaces

Configuring multiple virtual interfaces, or subinterfaces, on a single physical interface allows greater flexibility and connectivity on the network. A subinterface is a mechanism that allows a single physical interface to support multiple logical interfaces or networks. That is, several logical interfaces or networks can be associated with a single hardware interface. Subinterfaces are implemented in various WAN and LAN protocols, including ATM, Frame Relay, SMDS, X.25, and Novell IPX. For more information about using subinterfaces, refer to the appropriate protocol chapter.

Note The Cisco IOS software can support a maximum of 300 interfaces and subinterfaces.

Configure Features Available on any Interface

The following sections describe optional tasks that you can perform on any type of interface:

- Add a Description for an Interface
- Configure MOP
- Control Interface Hold-Queue Limits
- Set Bandwidth
- Set Interface Delay

- Adjust Timers
- Limit Transmit Queue Size
- Adjust Maximum Packet Size or MTU Size

Add a Description for an Interface

You can add a description about an interface to help you remember what is attached to it. This description is meant solely as a comment to help identify what the interface is being used for. The description will appear in the output of the following commands: **show configuration**, **show running-config**, and **show interfaces**. When you add a description for a T1 controller interface, it will appear in the output of the **show controllers t1** and **show running-config** commands.

To add a description for any interface but a T1 or E1 controller interface, perform the following task in interface configuration mode. To add a description for a T1 or E1 controller in a Cisco 4500 series, or Cisco 7200 series, or Cisco 7500 series routers, perform the following task in controller configuration mode:

Task	Command
Add a description for an interface.	**description** *string*

For examples of adding interface descriptions, see the section "Interface Description Examples" at the end of this chapter.

Configure MOP

You can enable MOP on an interface by performing the following task in interface configuration mode:

Task	Command
Enable MOP.	**mop enabled**

You can enable an interface to send out periodic MOP system identification messages on an interface by performing the following task in interface configuration mode:

Task	Command
Enable MOP message support.	**mop sysid**

Control Interface Hold-Queue Limits

Each interface has a hold-queue limit. This limit is the number of data packets that the interface can store in its hold queue before rejecting new packets. When the interface empties one or more packets from the hold queue, it can accept new packets again. You can specify the hold-queue limit of an interface in interface configuration mode as follows:

Task	Command
Specify the maximum number of packets allowed in the hold queue.	**hold-queue** *length* {**in** | **out**}

Set Bandwidth

Higher-level protocols use bandwidth information to make operating decisions. For example, IGRP uses the minimum path bandwidth to determine a routing metric. TCP adjusts initial retransmission parameters based on the apparent bandwidth of the outgoing interface. Perform the following task in interface configuration mode to set a bandwidth value for an interface:

Task	Command
Set a bandwidth value.	**bandwidth** *kilobits*

The bandwidth setting is a routing parameter only; it does not affect the physical interface.

Set Interface Delay

Higher-level protocols might use delay information to make operating decisions. For example, IGRP can use delay information to differentiate between a satellite link and a land link. To set a delay value for an interface, perform the following task in interface configuration mode:

Task	Command
Set a delay value for an interface.	**delay** *tens-of-microseconds*

Setting the delay value sets an informational parameter only; you cannot adjust the actual delay of an interface with this configuration command.

Adjust Timers

To adjust the frequency of update messages, perform the following task in interface configuration mode:

Task	Command
Adjust the frequency with which the Cisco IOS software sends messages to itself (Ethernet and Token Ring) or to the other end (HDLC-serial and PPP-serial links) to ensure that a network interface is alive for a specified interface.	**keepalive** [*seconds*]

You also can configure the *keepalive* interval, the frequency at which the Cisco IOS software sends messages to itself (Ethernet and Token Ring) or to the other end (HDLC-serial, PPP-serial), to ensure that a network interface is alive. The interval in some previous software versions was 10 seconds; it is now adjustable in one-second increments down to one second. An interface is declared down after three update intervals have passed without receiving a keepalive packet.

When adjusting the keepalive timer for a very low bandwidth serial interface, large packets can delay the smaller keepalive packets long enough to cause the line protocol to go down. You might need to experiment to determine the best value.

Limit Transmit Queue Size

You can control the size of the transmit queue available to a specified interface on the MCI and SCI cards. To limit the size, perform the following task in interface configuration mode:

Task	Command
Limit the size of the transmit queue.	**tx-queue-limit** *number*

Adjust Maximum Packet Size or MTU Size

Each interface has a default maximum packet size or maximum transmission unit (MTU) size. This number generally defaults to 1500 bytes. On serial interfaces, the MTU size varies, but cannot be set smaller than 64 bytes. To adjust the maximum packet size, perform the following task in interface configuration mode:

Task	Command
Adjust the maximum packet size or MTU size.	**mtu** *bytes*

Caution Changing an MTU size on a Cisco 7500 router will result in recarving of buffers and resetting of all interfaces. The following message is displayed:

```
%RSP-3-Restart:cbus complex
```

Understand Online Insertion and Removal (OIR)

The online insertion and removal (OIR) feature—supported on the Cisco 7200 series and the Cisco 7500 series routers only—allows you to remove and replace interface processors while the system is online. You can shut down the interface processor before removal and restart it after insertion without causing other software or interfaces to shut down.

Note Do not remove or install more that one interface processor at one time. After a removal or installation, observe the LEDs before continuing.

You do not need to notify the software that you are going to remove or install an interface processor. When the route processor is notified by the system that an interface processor has been removed or installed, it stops routing and scans the system for a configuration change. All interface processors are initialized, and each interface type is verified against the system configuration; then the system runs diagnostics on the new interface. There is no disruption to normal operation during interface processor insertion or removal.

Only an interface of a type that has been configured previously will be brought on line; others require configuration. If a newly installed interface processor does not match the system configuration, the interface is left in an administratively down state until the system operator configures the system with the new interfaces.

Hardware (MAC-level) addresses for all interfaces on the Cisco 7500 routers are stored on an electronically erasable programmable read-only memory (EEPROM) component in the Route Processor (RP) instead of on the individual interface boards. On the Cisco 7500, an address allocator in the EEPROM contains a sequential block of 40 addresses (5 interface slots times a maximum of

8 possible ports per slot; each address is assigned to a specific slot and port address in the chassis, regardless of how the interfaces are configured. On the Cisco 7200 series, hardware addresses are stored in a midplane EEPROM that supports 1024 addresses per box.

Storage of hardware addresses in EEPROM allows interfaces to be replaced online without requiring the system to update switching tables and data structures. Regardless of the types of interfaces installed, the hardware addresses do not change unless you replace the system RP. If you do replace the RP, the hardware addresses of *all* ports change to those specified in the address allocator on the new RP.

Understand Fast Switching Support

Switching is the process by which packets are forwarded. The Cisco IOS software supports multiple methods of switching. Cisco routers fast switch Layer 2 Forwarding (L2F) traffic. In stack group environments in which some L2F traffic is offloaded to a powerful router, fast switching provides improved scalability.

For information about switching features, refer to the *Cisco IOS Switching Services Configuration Guide*. For documentation of commands used to configure switching features, refer to the *Cisco IOS Switching Services Command Reference*.

Monitor and Maintain the Interface

You can perform the tasks in the following sections to monitor and maintain the interfaces:

- Monitor Interface and Controller Status
- Monitor the T1 or E1 Controller
- Monitor and Maintain CSU/DSU Service Modules
- Monitor the LAN Extender Interface
- Monitor and Maintain a Hub
- Monitor Tunnels
- Clear and Reset the Interface
- Shut Down and Restart the Interface
- Configure Loopback Detection
- Run Interface Loopback Diagnostics
- Enable Loopback Testing of Fractional T1/T1

Monitor Interface and Controller Status

The software contains commands that you can enter at the EXEC prompt to display information about the interface including the version of the software and the hardware, the controller status, and statistics about the interfaces. The following table lists some of the interface monitoring tasks. (You can display the full list of **show** commands by entering the **show ?** command at the EXEC prompt.) These commands are fully described in the *Configuration Fundamentals Command Reference*.

Perform the following commands in EXEC mode:

Task	Command
Display the status of the asynchronous interface.	**show async status** **show interfaces async**
Display compression statistics on a serial interface.	**show compress**
Display current internal status information for the interface controller cards.	**show controllers** [{**bri** | **cbus** | **fddi** | **lance** | **mci** | **serial** | **token**}]
Display information about the Switch Processor (SP) controller on the Cisco 7500 series.	**show controllers cbus**
Display current internal status information for the interface controller cards.	**show controllers** [{**e1** | **ethernet** | **fastethernet** | **fddi** | **serial** | **t1** | **token**}]
Display current internal status information for the interface controller cards on the Cisco 7200 and Cisco 7500 series routers,	**show controllers** {**ethernet** | **fastethernet** | **fddi** | **serial** | **token**}
Display diagnostic information about the controller, interface processor, and port adapters associated with a specified slot of a Cisco 7200 series, or Cisco 7500 series router.	**show diagbus** [*slot*]
If accounting is configured, display the number of packets of each protocol type that have been sent through the interface. For Cisco 7500 series with a Packet over SONET Interface Processor.	**show interfaces** [*type number*] [*first*] [*last*] [**accounting**] **show interfaces** [*type slot*/*port*] [**accounting**]
For the Cisco 7500 series with VIP or VIP2 cards.	**show interfaces** [*type slot*/*port-adapter*/*port*] [**accounting**]
Display information about the Cisco 7500 with a Packet over SONET Interface Processor.	**show interfaces posi** [*slot*/*port*]
Display the number of packets of each protocol type that have been sent through the asynchronous serial line.	**show interfaces async** [*number*] [**accounting**]
Display the currently running configuration in RAM.	**show running-config**
Display the current contents of the routing information field (RIF) cache.	**show rif**
Display the global (system-wide) and interface-specific status of any configured Level 3 protocol.	**show protocols**
Display the hardware configuration, software version, the names and sources of configuration files, and the boot images.	**show version**

Monitor the T1 or E1 Controller

This section applies to channelized T1 or E1 interfaces. Because the T1 or E1 link itself is viewed as the controller, perform the following task in EXEC mode to display information about activity on the T1 or E1 line.

Task	Command
Display information about the T1 link.	**show controller t1**

Task	Command
Display information about the E1 link.	**show controller e1**

Alarms, line conditions, and other errors are displayed. The data is updated every 10 seconds. Every 15 minutes, the cumulative data is stored and retained for 24 hours. This means at any one time, up to 96 15-minute accumulations are counted in the data display.

Monitor and Maintain CSU/DSU Service Modules

This section describes how to monitor and maintain service modules. Tasks involved to monitor and maintain service modules are described in these sections:

- Perform a Self-Test
- Display a Performance Report
- Perform Loopback Tests
- Reset the CSU/DSU

Perform a Self-Test

To perform a self-test on the integrated CSU/DSU, perform the following task in privileged EXEC mode:

Task	Command
Perform a self test. Specify the interface type and number.	**test service-module** *interface*

This command cannot be used if a DTE, line, or remote loopback is in progress. 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. This self-test is also performed at power on.

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

Display a Performance Report

To display the performance report for an integrated CSU/DSU, perform one of the following tasks in privileged EXEC mode:

Tasks	Command
Display a performance report. Choose either serial interface 1 or 0.	**show service-module** *interface*
Display the CSU/DSU performance statistics for the past 24 hours. This command applies only to the FT1/T1 module.	**show service-module** *interface* **performance-statistics** [*interval-range*]

The *interval-range* value specifies the number of 15-minute intervals displayed in the report. 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.

Perform Loopback Tests

You can loop packets back to the network from the integrated CSU/DSU and loop packets through a local CSU/DSU to a remote CSU/DSU.

Perform Loopback Line Test

To loop data received from the line at the integrated CSU/DSU and loop packets back to the line, perform the following tasks in interface configuration mode:

Task	Command
Perform loopback at a point close to the network to CSU/DSU interface.	**loopback line**
Perform loopback at a point close to the interface between the CSU/DSU and the router.	**loopback line payload**

Packets are looped from an incoming network transmission back into the network at a CSU or DSU loopback point.

When the **loopback line** command is configured on the 2-wire 56-kbps CSU/DSU module or the 4-wire 56/64-kbps CSU/DSU modules installed on a Cisco 2524 or Cisco 2525 router, the network data loops back at the CSU and the router data loops back at the DSU. If the CSU/DSU is configured for switched mode, you must have an established connection to perform a payload-line loopback. When the **loopback line payload** command is configured, the CSU/DSU module loops the data through the DSU portion of the module. Data is not looped back to the serial interface.

If you enable the **loopback line** command on the fractional T1/T1 module, the CSU/DSU performs a full-bandwidth loopback through the CSU portion of the module and data transmission through the serial interface is interrupted for the duration of the loopback. No reframing or corrections of bipolar violation errors or cyclic redundancy check (CRC) errors are performed. When you configure the **line loopback payload** command on the FT1/T1 module, the CSU/DSU performs a loopback through the DSU portion of the module. The **line loopback payload** command reframes the data link, regenerates the signal, and corrects bipolar violations and Extended Super Frame CRC errors.

When performing a T1-line loopback with Extended Super Framing, communication over the facilities data link is interrupted but performance statistics are still updated. To show interfaces currently in loopback operation, use the **show service-module** EXEC command.

Perform Loopback DTE

To loop packets back to DTE from within the local CSU/DSU, perform the following task:

Task	Command
Loop packets to DTE.	**loopback dte**

Packets are looped from within the CSU/DSU back to the serial interface of the router. Send a test ping to see if the packets successfully looped back. To cancel the loopback test, use the **no loopback dte** command.

When using the 4-wire 56/64-kbps CSU/DSU module, an out-of-service signal is transmitted to the remote CSU/DSU.

Perform a Remote Loopback Test Using the FT1/T1 CSU/DSU Module

This command applies only when the remote CSU/DSU device is configured for this function. It is used for testing the data communication channels along with or without remote CSU/DSU circuitry. The loopback is usually performed at the line port, rather than the DTE port, of the remote CSU/DSU.

On the integrated FT1/T1 CSU/DSU module installed on a Cisco 2524 and Cisco 2525 router, the **loopback remote full** command sends the loopup code to the remote CSU/DSU. The remote CSU/DSU should perform a full-bandwidth loopback through the CSU portion of the module. The **loopback remote payload** command sends the loopup code on the configured timeslots, while maintaining the D4-ExtendedSuper Framing. The remote CSU/DSU performs the equivalent of a loopback line payload request. The remote CSU/DSU loops back only those timeslots that are configured of the remote end. This loopback reframes the data link, regenerates the signal, and corrects bipolar violations and Extended Super Frame CRC errors. The **loopback remote smart-jack** command sends a loopup code to the remote smart jack. You cannot put the local smart jack into loopback.

To loop packets on the integrated FT1/T1 CSU/DSU module, perform the following task:

Task	Command
Loop packets at a remote CSU/DSU using the fractional T1/T1 CSU/DSU module.	**loopback remote** {**full** | **payload** | **smart-jack**} [**0in1** | **1in1** | **1in2** | **1in5** | **1in8** | **3in24** | **qrw** | **user-pattern** *24bit-binary value*]

Failure to loop up or initiate a remote loopback request could be caused by enabling the **no service-module t1 remote-loopback** command or having an alternate remote-loopback code configured on the remote end. When the loopback is terminated, the result of the pattern test is displayed.

Note If the FT1/T1 CSU/DSU module is configured to provide internal clocking, the module ceases to generate clocking when it is placed into loopback.

2- and 4-Wire 56/64-kbps CSU/DSU Modules

This command applies only when the remote CSU/DSU device is configured for this function. It is used for testing the data communication channels along with or without remote CSU/DSU circuitry. The loopback is usually performed at the line port, rather than the DTE port, of the remote CSU/DSU.

On the 2- and 4-wire 56/64-kbps CSU/DSU modules, an active connection is required before a loopup can be initiated while in switched mode. When transmitting V.54 loopbacks, the remote device is commanded into loopback using V.54 messages. Failure to loop up or initiate a remote loopback request could be caused by enabling the **no service-module 56k remote-loopback** command.

To loop packets at the remote CSU/DSU, perform the following task:

Task	Command
Loop packets at a remote CSU/DSU using the 2- and 4-wire 56/64-kbps CSU/DSU modules.	**loopback remote** [**2047** | **511** | **stress-pattern** *pattern number*]

To show interfaces currently in loopback operation, use the **show interfaces loopback** EXEC command.

Reset the CSU/DSU

To reset the CSU/DSU, perform the following task in privileged EXEC mode:

Task	Command
Reset the CSU/DSU. Specify the interface type and number.	**clear service-module** *interface*

Use this command only in severe circumstances (for example, when the router is not responding to a CSU/DSU configuration command).

This command terminates all DTE and line loopbacks that are locally or remotely configured. It also interrupts data transmission through the router for up to 15 seconds. The software performs an automatic software reset in case of two consecutive configuration failures.

The CSU/DSU module is not reset with the **clear interface** command.

Caution If you experience technical difficulties with your router and intend to contact customer support, refrain from using this command. The command erases the router's past CSU/DSU performance statistics. To clear only the CSU/DSU performance statistics, issue the **clear counters** command.

Monitor the LAN Extender Interface

To monitor the LAN Extender interface, the Ethernet interface that resides on the LAN Extender, the serial interface that resides on the LAN Extender, or the serial interface connected to the LAN Extender, perform one or more of the following tasks at the EXEC prompt:

Task	Command
Display hardware and software information about the LAN Extender.	**show controllers lex** [*number*]
Display information on the Cisco 7500 series.	**show controllers lex** [*slot*/*port*]
Display statistics about the LAN Extender interface.	**show interfaces lex** *number* [**ethernet** | **serial**]
Display statistics about the serial interface on the host router that is physically connected to the LAN Extender.	**show interfaces serial** *number* [**accounting**]
Display statistics on the Cisco 7500 series.	**show interfaces serial** *slot*/*port* [**accounting**]

For more complete network troubleshooting information, refer to the *Troubleshooting Internetworking Systems* publication.

Monitor and Maintain a Hub

You can perform the tasks in the following sections to monitor and maintain the hub:

- Shut Down the Hub Port
- Reset the Hub or Clear the Hub Counters
- Monitor the Hub

Shut Down the Hub Port

To shut down or disable a hub port, perform the following tasks, beginning in global configuration mode:

Task	Command
Specify the hub number and the hub port (or range of hub ports) and place you in hub configuration mode.	**hub ethernet** *number port* [*end-port*]
Shut down the hub port.	**shutdown**

See the examples of shutting down a hub port at the end of the "Configuring LAN Interfaces" chapter in "Hub Configuration Examples."

Reset the Hub or Clear the Hub Counters

To reset the hub or clear the hub counters, perform one of the following tasks in EXEC mode:

Task	Command
Reset and reinitialize the hub hardware.	**clear hub ethernet** *number*
Clear the hub counters displayed by the **show hub** command.	**clear hub counters** [**ethernet** *number* [*port* [*end-port*]]]

Monitor the Hub

To display hub information, perform the following task in EXEC mode:

Task	Command
Display hub statistics.	**show hub** [**ethernet** *number* [*port* [*end-port*]]]

Monitor Tunnels

Complete any of the following tasks in EXEC mode to monitor the IP tunnels you have configured:

Task	Command
List tunnel interface information.	**show interfaces tunnel** *unit* [**accounting**]
List the routes that go through the tunnel.	**show** *protocol* **route**
List the route to the tunnel destination.	**show ip route**

Clear and Reset the Interface

To clear the interface counters shown with the **show interfaces** command, enter the following command at the EXEC prompt:

Task	Command
Clear the interface counters.	**clear counters** [*type number*] [**ethernet** | **serial**]
Clear interface counters for the FastEthernet NIM on the Cisco 4000 series or Cisco 4500 series.	**clear counters fastethernet** *number*
Clear interface counters for the Cisco 7200 series.	**clear counters** [*type slot*/*port*]
Clear interface counters for the Cisco 7500 series with VIP or VIP2 Interface Processors.	**clear counters** [*type slot*/*port-adaptor*]

The command clears all the current interface counters from the interface unless the optional arguments are specified to clear only a specific interface type from a specific slot and port number.

Note This command will not clear counters retrieved using SNMP, but only those seen with the EXEC **show interfaces** command.

Complete the following tasks in EXEC mode to clear and reset interfaces. Under normal circumstances, you do not need to clear the hardware logic on interfaces.

Task	Command
Reset the hardware logic on an interface.	**clear interface** *type number*
Reset the hardware logic on an asynchronous serial line.	**clear line** [*number*]
Clear the entire Token Ring RIF cache.	**clear rif-cache**

Shut Down and Restart the Interface

You can disable an interface. Doing so disables all functions on the specified interface and marks the interface as unavailable on all monitoring command displays. This information is communicated to other network servers through all dynamic routing protocols. The interface will not be mentioned in any routing updates. On serial interfaces, shutting down an interface causes the DTR signal to be dropped. On Token Ring interfaces, shutting down an interface causes the interface to deinsert from the ring. On FDDIs, shutting down an interface causes the optical bypass switch, if present, to go into bypass mode.

To shut down an interface and then restart it, perform the following tasks in interface configuration mode:

Command	Task
Shut down an interface.	**shutdown**
Reenable an interface.	**no shutdown**

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 **show interfaces** command display. See examples in the section "Interface Shutdown Examples" at the end of this chapter.

One reason to shut down an interface is if you want to change the electrical interface type or mode of a Cisco 7500 series port online. You replace the serial adapter cable and use software commands to restart the interface, and if necessary, reconfigure the port for the new interface. At system startup or restart, the FSIP polls the interfaces and determines the electrical interface type of each port (according to the type of port adapter cable attached). However, it does not necessarily repoll an interface when you change the adapter cable online. To ensure that the system recognizes the new interface type, shut down using the **shutdown** command, and reenable the interface after changing the cable. Refer to your hardware documentation for more details.

Configure Loopback Detection

When an interface has a backup interface configured, it is often desirable that the backup interface be enabled when the primary interface is either down or in loopback. By default, the backup is only enabled if the primary interface is down. By using the **down-when-looped** command, the backup interface will also be enabled if the primary interface is in loopback. To achieve this condition, perform the following task in interface configuration mode:

Task	Command
Configure an interface to tell the system it is down when loopback is detected.	**down-when-looped**

If testing an interface with the loopback command, you should not have loopback detection configured, or packets will not be transmitted out the interface that is being tested.

Run Interface Loopback Diagnostics

You can use a loopback test on lines to detect and distinguish equipment malfunctions between line and modem or Channel Service Unit/Digital Service Unit (CSU/DSU) problems on the network server. If correct data transmission is not possible when an interface is in loopback mode, the interface is the source of the problem. The DSU might have similar loopback functions you can use to isolate the problem if the interface loopback test passes. If the device does not support local loopback, this function will have no effect.

You can specify hardware loopback tests on the Ethernet and synchronous serial interfaces, and all Token Ring interfaces that are attached to CSU/DSUs and that support the local loopback signal. The CSU/DSU acts as a Data Communications Equipment (DCE) device; the router or access server acts as a Data Terminal Equipment (DTE) device. The local loopback test generates a CSU loop—a signal that goes through the CSU/DSU to the line, then back through the CSU/DSU to the router or access server. The **ping** command can also be useful during loopback operation.

The loopback tests are available on the following interfaces:

- High-Speed Serial Interface (HSSI), including the High-Speed Communications Interface (HSCI) card ribbon cable
- Cisco Multiport Communications Interface (MCI) and Cisco Serial Communication Interface (SCI) synchronous serial interfaces
- MCI and Cisco Multiport Ethernet Controller (MEC) Ethernet interfaces; an Ethernet loopback server is also provided on the Ethernet interfaces
- Ethernet loopback server

- Channelized E1 interfaces (local loopback only)
- Channelized T1 interfaces (local and remote loopback)
- Fractional T1/T1 Interfaces
- Token Ring interfaces
- Channelized E1 controller and interface (local loopback only)
- Channelized T1 controller and interface (local and remote loopback)
- Troubleshooting channelized E1 and channelized T1

The following sections describe each test.

Note Loopback does not work on an X.21 DTE because the X.21 interface definition does not include a loopback definition.

Enable Loopback Testing on the HSSI

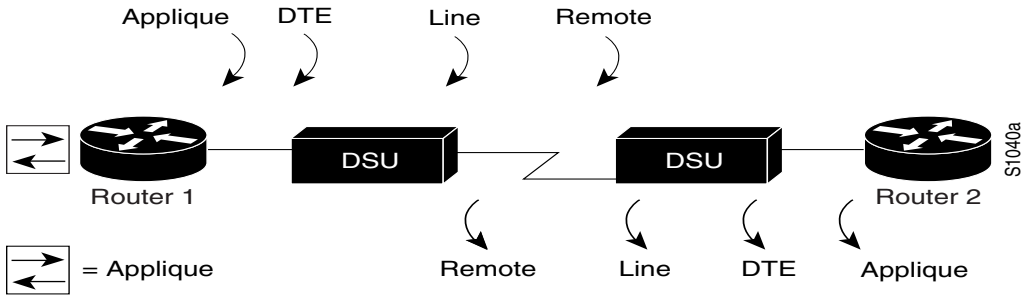
The HSSI allows you to perform the tasks described in these sections:

- Enable Loopback Test to the DTE
- Enable Loopback Test through the CSU/DSU
- Enable Loopback Test over Remote DS-3 Link

These tests apply only when the device supports them and are used to check the data communications channels. The tests are usually performed at the line port rather than the DTE port of the remote CSU/DSU.

The internal loopback concepts are illustrated in Figure 18.

Figure 18 HSSI Loopback Testing



Enable Loopback Test to the DTE

You can loop packets to DTE within the CSU/DSU at the DTE interface, when the device supports this function. Doing so is useful for testing the DTE-to-DCE cable. To loop the packets to DTE, perform the following task in interface configuration mode:

Task	Command
Loop packets to DTE internally.	**loopback dte**

Enable Loopback Test through the CSU/DSU

You can loop packets completely through the CSU/DSU to configure a CSU loop, when the device supports this feature. Doing so is useful for testing the DCE device (CSU/DSU) itself. To configure a CSU loop, perform the following task in interface configuration mode:

Task	Command
Loop packets completely through the CSU/DSU.	**loopback line**

Enable Loopback Test over Remote DS-3 Link

You can loop packets through the CSU/DSU, over the Digital signal level 3 (DS-3) link, and to the remote CSU/DSU and back. To do so, perform the following task in interface configuration mode:

Task	Command
Loop packets through the CSU/DSU to a remote CSU/DSU over the DS-3 link.	**loopback remote**

This command applies only when the device supports the remote function. It is used for testing the data communication channels. The loopback usually is performed at the line port, rather than the DTE port, of the remote CSU/DSU.

Configure the Ethernet Loopback Server

The router software provides an Ethernet loopback server that supports Digital Equipment Corporation (Digital), Intel, and Xerox systems specified by the "blue book," a joint specification written by Digital, Intel, and Xerox that defines the Ethernet protocol. The loopback server responds to forward data loopback messages sent either to the server's MAC address or to the broadcast address. Currently, the Ethernet loopback server does not respond to the loopback assistance multicast address.

Use the Ethernet loopback server to test communications between your internetworking products and Digital systems that do not support the IP **ping** command, such as DECnet-only VMS systems.

To originate a loop test on your VMS system with a Cisco server, use the Digital Network Control Program (NCP) command **loop circuit**. For more information about the **loop circuit** command, consult the DECnet VAX documentation. Cisco network servers support all options that can be specified by the VMS hosts.

Enable Loopback on Token Ring Cards

You can place all of the Token Ring interface cards into loopback mode by performing the following task in interface configuration mode:

Task	Command
Enable loopback to verify that the Token Ring interface receives back every packet it sends.	**loopback**

Enable Loopback Testing of Fractional T1/T1

For information, see the "Perform Loopback Tests" in the "Monitor and Maintain CSU/DSU Service Modules" section earlier in this chapter.

Interface Configuration Examples

Examples are included in this section to illustrate configuration tasks described in this chapter. These configuration examples are provided:

- Enable Interface Configuration Examples
- Interface Description Examples
- Interface Shutdown Examples

Enable Interface Configuration Examples

The following example illustrates how to begin interface configuration on a serial interface. It assigns Point-to-Point (PPP) encapsulation to serial interface 0.

```
interface serial 0
encapsulation ppp
```

Configure Specific IP Addresses for an Interface Example

This example shows how to configure the access server so that it will use the default address pool on all interfaces except interface 7, on which it will use an address pool called lass:

```
ip address-pool local
ip local-pool lass 172.30.0.1
 async interface
 interface 7
 peer default ip address lass
```

Interface Description Examples

The following example illustrates how to add a description about an interface that will appear in configuration files and monitoring command displays:

```
interface ethernet 0
description First Ethernet in network 1
ip address 101.13.15.78 255.255.255.0
```

The following example for a Cisco 7500 describes an administration network attached to the Ethernet processor in slot 2, port 4:

```
interface ethernet 2/4
description 2nd floor administration net
```

Interface Shutdown Examples

The following example turns off the Ethernet interface in slot 2 at port 4:

```
interface ethernet 2/4
shutdown
```

The following example turns the interface back on:

```
interface ethernet 2/4
no shutdown
```

The following example illustrates how to shut down a Token Ring interface:

```
interface tokenring 0
shutdown
```

The following example shuts down a T1 circuit number 23 running on a Cisco 7500:

```
interface serial 4/0:23
shutdown
```

The following example shuts down the entire T1 line physically connected to a Cisco 7500:

```
controller t1 4/0
shutdown
```