Doc. No. 78-3799-01

Cisco IOS Release 11.1 CA Release Note and Update to Configuration Guides and Command References

October 7, 1996

This document describes the features and caveats for Cisco Internetwork Operating System (Cisco IOS) Release 11.1 CA, up to and including Release 11.1(6)CA. Release 11.1(6)CA is a platform-specific software release that supports new features for the Cisco 7000 series routers with RSP7000, Cisco 7200 series routers, and Cisco 7500 series routers not available in Cisco IOS Release 11.1(6). This document supplements the Cisco IOS Release 11.1 documentation set with new and changed commands that support the new features in Release 11.1(6)CA.

This document will be updated as additional releases of Release 11.1 CA are made available to support new hardware and software features.

This document is divided into the following sections:

Corporate Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA

Use this document in conjunction with the *Release Notes for Cisco IOS Release 11.1* and the Cisco IOS Release 11.1 configuration guide and command reference publications, specifically the *Configuration Fundamentals Configuration Guide* and *Configuration Fundamentals Command Reference*.

Release Note

The release note portion of this document describes the platforms supported, packaging, boot ROM requirements, memory requirements, features, and caveats for Cisco IOS Release 11.1(6)CA.

Platform Support

Cisco IOS Release 11.1(6)CA supports the following platforms:

- Cisco 7000 series routers with RSP7000
- Cisco 7200 series routers
- Cisco 7500 series routers

Refer to the *Release Notes for Cisco IOS Release 11.1* publication for a summary of the LAN interfaces supported on each platform and the WAN data rates and interfaces supported on each platform.

Cisco IOS Packaging

The following feature sets are available in Release 11.1 CA for the Cisco 7000 series routers with RSP7000, Cisco 7200 series routers, and Cisco 7500 series routers. Refer to *Release Notes for Cisco IOS Release 11.1* for a complete list of the features provided in these sets.

For the Cisco 7000 series routers with RSP7000 and Cisco 7500 series routers:

- Enterprise
- Enterprise/APPN
- Enterprise/VIP

- Enterprise/APPN/VIP
- Source Route Switch (Cisco 7000 series only)

For the Cisco 7200 series routers:

- Enterprise
- Enterprise/APPN
- Desktop/IBM
- Network Layer 3 Switching

Boot ROM Requirements

The Cisco 7200 series requires a boot image of level 11.1(472), 11.1(5a), or later.

The VIP2 requires a boot image of level 11.1(472), 11.1(5a), or later.

Memory Requirements

Refer to the *Release Notes for Cisco IOS Release 11.1* publication for the memory requirements for feature sets available in Release 11.1(6)CA.

Note The Cisco 7500 series requires a 16- or 20-MB Flash memory card to support the Enterprise/APPN/VIP feature set and the CIP microcode.

New Features in Release 11.1(6)CA

The following new features have been added to Release 11.1(6)CA:

- To improve performance, fragmented IP packets are now optimum or flow switched (depending which switching method is enabled) rather than being process switched on Cisco 7000 series with RSP7000 and Cisco 7500 series routers.
- High System Availability (HSA) is now supported when a Versatile Interface Processor (VIP) or second-generation VIP (VIP2) is installed in the Cisco 7507 and Cisco 7513 routers. HSA is an advanced software feature that increases the availability and uptime of these routers. This increase is accomplished through a master/slave relationship between two RSP2s. If the slave RSP2 detects an error condition, it automatically takes control and reboots the router without user intervention. This automatic action minimizes network interruption and increases system availability. For more information and important notes on HSA, refer to the *Release Notes for Cisco IOS Release 11.1*.
- Source route bridging (SRB) over FDDI is now supported on the Cisco 7200 series routers.
- Support for the following new port adapters and service adapters:
  - PA-F/FD-SM and PA-F/FD-MM FDDI full-duplex single-mode and multimode port adapters on the second-generation Versatile Interface Processor (VIP2) in all Cisco 7500 series routers and on the Cisco 7000 series routers using the 7000 Series Route Switch Processor (RSP7000) and 7000 Series Chassis Interface (RSP7000CI). These port adapters provide an interface for both single-mode and multimode fiber-optic cable. The two physical

ports are available with either single-mode SC-type or multimode MIC receptacles. Each port adapter's FDDI connection allows a maximum bandwidth of 100 Mbps per the FDDI standard.

— PA-H and PA-2H HSSI port adapters provide up to two high-speed serial interfaces on the Cisco 7200 series routers, on the VIP2 in all 7500 series routers, and on the Cisco 7000 series routers using the RSP7000 and RSP7000CI. These port adapters support a full-duplex synchronous serial interface for transmitting and receiving data at rates up to 52 Mbps.

— PA-8T-V35 synchronous serial port adapter provides up to eight synchronous serial interfaces on the Cisco 7200 series routers, on the VIP2 in all 7500 series routers, and on the Cisco 7000 series routers using the RSP7000 and RSP7000CI. This port adapter supports full-duplex operation at T1 (1.544 Mbps) and E1 (2.048 Mbps) speeds.

— SA-Comp/1 and SA-Comp/2 data compression service adapters provide high-performance, hardware-based data compression capabilities on the Cisco 7200 series routers, on the VIP2 in all 7500 series routers, and on the Cisco 7000 series routers using the RSP7000 and RSP7000CI. These service adapters support simultaneous Stacker compression data compression algorithms with independent full-duplex compression and decompression capabilities on point-to-point (PPP) encapsulation packets.

  The compression service adapters can be monitored with the Cisco Compression Service Adapter (CSA) MIB. For information on accessing Cisco MIB files, refer to the *Cisco MIB User Quick Reference.*

Release 11.1(6)CA Caveats

Refer to the *Release Notes for Cisco IOS Release 11.1* publication for a list of the caveats that apply to Release 11.1(6). The caveats that apply to Cisco IOS Release 11.1(6) apply to Release 11.1(6)CA. Release 11.1(6)CA has no specific caveats for the new features in this software release.

If you have an account on CCO, you can view additional caveats using the bug search tools in the Bug Toolkit, such as the Bug Navigator.

Update to Configuration Guides

The information in the sections below supplements the *Configuration Fundamentals Configuration Guide*. Pointers to sections and page numbers are shown in *italic* typeface.

Configuring Interfaces

On page 194 of the "Configuring Interfaces" chapter of the Cisco IOS Release 11.1 Configuration Fundamentals Configuration Guide, add the following new "Enable Full-Duplex" section after the "Preallocate Buffers for Bursty FDDI Traffic" section:

Enable Full-Duplex

To enable full-duplex mode on the FDDI full-duplex, single mode port adapter (PA-F/FD-SM) and FDDI full-duplex, multimode port adapter (PA-F/FD-MM) on the Cisco 7000 series routers with RSP7000 and the Cisco 7500 series routers, perform the following task in interface configuration mode:

Task	Command
Enable full-duplex on the FDDI interface of the PA-F/FD-SM and PA-F/FD-MM port adapter.	**fddi full-duplex**

On page 215 of the "Configuring Interfaces" chapter of the Cisco IOS Release 11.1 Configuration Fundamentals Configuration Guide, replace the "Configure Compression of PPP Data" section with the section shown below:

Configure Compression of PPP Data

You can configure point-to-point compression on serial interfaces that use PPP encapsulation. Compression reduces the size of a PPP frame via lossless data compression. PPP encapsulations support both predictor and Stacker compression algorithms.

If the majority of your traffic is already compressed files, do not use compression.

When you configure Stacker compression on the Cisco 7000 series routers with RSP7000, Cisco 7200 series routers, and Cisco 7500 series routers, there are three methods of compression. Specifying the **compress stac** command with no options causes the router to use the fastest available compression method:

- If the router contains a compression service adapter (CSA), compression is performed in the CSA hardware (hardware compression).
- If the CSA is not available, compression is performed in the software installed on the VIP2 (distributed compression).
- If the VIP2 is not available, compression is performed in the router's main processor (software compression).

Using hardware compression in the CSA frees the router's main processor for other tasks. You can also configure the router to use the VIP2 to perform compression by using the **distributed** option, or to use the router's main processor by using the **software** option. If the VIP2 is not available, compression is performed in the router's main processor.

When compression is performed in software installed in the router's main processor, it might significantly affect system performance. Cisco recommends that you disable compression in the router's main processor if the router CPU load exceeds 40 percent. To display the CPU load, use the **show process cpu** EXEC command.

To configure compression over PPP, perform the following tasks in interface configuration mode:

Task		Command
Step 1	Enable encapsulation of a single protocol on the serial line.	**encapsulation ppp**
Step 2	Enable compression.	**compress** {**predictor** | **stac**} or **compress** {**predictor** | **stac** [**distributed** | **software**]} (Cisco 7000 series routers with RSP7000 and Cisco 7500 series routers) or **compress** {**predictor** | **stac** [**software**]} (Cisco 7200 series routers)

On page 217 of the "Configuring Interfaces" chapter of the Cisco IOS Release 11.1 Configuration Fundamentals Configuration Guide, replace the "Use the NRZ Line-Coding Format" section with the section shown below:

Use the NRZI Line-Coding Format

All FSIP interface types on the Cisco 7000 and the PA-8T synchronous serial port adapter on the Cisco 7000 series routers with RSP7000, Cisco 7200 series routers, and Cisco 7500 series routers support nonreturn-to-zero (NRZ) and nonreturn-to-zero inverted (NRZI) format. This is a line-coding format that is required for serial connections in some environments. NRZ encoding is most common. NRZI encoding is used primarily with EIA/TIA-232 connections in IBM environments.

The default configuration for all serial interfaces is NRZ format. The default is **no nrzi-encoding**. To enable NRZI format, complete the following task in interface configuration mode:

Task	Command
Enable NRZI encoding format.	**nrzi-encoding** or **nrzi-encoding** [**mark**] (Cisco 7000 series routers with RSP7000, Cisco 7200 series routers, and Cisco 7500 series routers)

On page 218 of the "Configuring Interfaces" chapter of the Cisco IOS Release 11.1 Configuration Fundamentals Configuration Guide, replace the "Invert the Transmit Clock Signal" section with the section shown below:

Invert the Transmit Clock Signal

Systems that use long cables or cables that are not transmitting the TxC signal (transmit echoed clock line, also known as TXCE or SCTE.clock) can experience high error rates when operating at the higher transmission speeds. For example, if the interface on the PA-8T synchronous serial port adapter is reporting a high number of error packets, a phase shift might be the problem. Inverting the clock signal may correct this shift. To invert the clock signal, complete the following task in interface configuration mode:

Task	Command
Invert the clock signal on an interface.	**invert txclock**

On page 218 of the "Configuring Interfaces" chapter of the Cisco IOS Release 11.1 Configuration Fundamentals Configuration Guide, add the following new "Invert the Data" section after the "Invert the Transmit Clock Signal" section:

Invert the Data

If the interface on the PA-8T synchronous serial port adapter is used to drive a dedicated T1 line that does not have B8ZS encoding, you must invert the data stream on the connecting CSU/DSU or on the interface. Be careful not to invert data on both the CSU/DSU and the interface as two data inversions will cancel each other out. To invert the data stream, complete the following task in interface configuration mode:

Task	Command
Invert the data on an interface.	**invert data**

Update to Command References

Commands in the “Interface Commands” chapter of the *Configuration Fundamentals Command Reference* publication have been added and changed. Refer to the Cisco IOS Release 11.1 configuration guide and command reference publications for additional commands.

- **compress**—this command was modified to include new options for the compression service adapter (CSA) on the Cisco 7000 series routers with RSP7000, Cisco 7500 series routers, and Cisco 7200 series routers
- **fddi full-duplex—**this command was added to support full-duplex on the FDDI full-duplex, single mode-to-multimode port adapter (PA-F/FD-SM) and FDDI full-duplex, multimode-to-multimode port adapter (PA-F/FD-MM) on the Cisco 7000 series routers with RSP7000 and Cisco 7500 series routers
- **invert data**—this command was added to support the PA-8T synchronous serial port adapter on the Cisco 7000 series routers with RSP7000, Cisco 7200 series routers, and Cisco 7500 series routers
- **invert txclock**—this command was modified to change the command syntax from invert-transmit-clock to invert txclock
- **nrzi-encoding**—this command was modified to add an option to support the PA-8T synchronous serial port adapter and PA-H and PA-2H HSSI port adapter on the Cisco 7000 series routers with RSP7000, Cisco 7200 series routers, and Cisco 7500 series routers
- **show compress—**this command was modified to include sample output using hardware compression on the compression service adapter (CSA) on the Cisco 7000 series routers with RSP7000, Cisco 7500 series routers, and Cisco 7200 series routers
- **show interfaces fddi—**this command was modified to show output for the FDDI full-duplex, single mode-to-multimode port adapter (PA-F/FD-SM) and FDDI full-duplex, multimode-to-multimode port adapter (PA-F/FD-MM) on the Cisco 7000 series routers with RSP7000 and Cisco 7500 series routers

compress

To configure compression for Link Access Procedure, Balanced (LAPB), Point-to-Point Protocol (PPP), and High-Level Data Link Control (HDLC) encapsulations, use the **compress** interface configuration command. On the Cisco 7000 series routers with RSP7000, Cisco 7500 series routers, and Cisco 7200 series routers, hardware compression on the compression service adapter (CSA) is supported for PPP links. To disable compression, use the **no** form of this command.

compress {**predictor** | **stac**}
no compress {**predictor** | **stac**}

compress {**predictor** | **stac** [**distributed** | **software**]} (Cisco 7500 series and Cisco 7000 series routers with RSP7000)
compress {**predictor** | **stac** [**software**]} (Cisco 7200 series routers)

Syntax Description

predictor	Specifies that a predictor (RAND) compression algorithm will be used on LAPB and PPP encapsulation. Compression is implemented in the software installed in the router's main processor.
stac	Specifies that a Stacker (LZS) compression algorithm will be used on LAPB, HDLC, and PPP encapsulation. For all platforms except Cisco 7200 series and platforms that support the VIP2, compression is implemented in the software installed in the router's main processor. On the Cisco 7200 series and on VIP2s in all Cisco 7500 series and Cisco 7000 series routers with RSP7000, specifying the **compress stac** command with no options causes the router to use the fastest available compression method for PPP encapsulation only: • If the router contains a compression service adapter (CSA), compression is performed in the CSA hardware (hardware compression). • If the CSA is not available, compression is performed in the software installed on the VIP2 (distributed compression). • If the VIP2 is not available, compression is performed in the router's main processor (software compression).
distributed	(Optional) Specifies that compression is implemented in the software that is installed in a VIP2. If the VIP2 is not available, compression is performed in the router's main processor (software compression).
software	(Optional) Specifies that compression is implemented in the Cisco IOS software installed in the router's main processor.

Default

Compression is disabled.

Command Mode

Interface configuration

Usage Guidelines

Using CSA hardware compression on the Cisco 7000 series routers with RSP7000, Cisco 7200 series routers, and Cisco 7500 series routers removes the compression and decompression responsibilities from the VIP2 or the main processor installed in the router. By using the **compress stac** command, the router determines the fastest compression method available on the router.

You can configure point-to-point software compression for all LAPB, PPP, and HDLC encapsulations. Compression reduces the size of frames via lossless data compression. HDLC encapsulations supports the Stacker compression algorithm. PPP and LAPB encapsulations support both predictor and Stacker compression algorithms.

When compression is performed in software installed in the router's main processor, it may significantly affect system performance. We recommend that you disable compression if the CPU load exceeds 40 percent. To display the CPU load, use the **show process cpu** EXEC command.

Compression requires that both ends of the serial link be configured to use compression.

If the majority of your traffic is already compressed files, we recommend that you not use compression. If the files are already compressed, the additional processing time spent in attempting unsuccessfully to compress them again will slow system performance.

Table 1 provides general guidelines for deciding which compression type to select.

Table 1 Compression Guidelines

Situation	Compression Type to Use
The bottleneck is caused by the load on the router.	Predictor
The bottleneck is the result of line bandwidth or hardware compression on the CSA is available.	Stacker
Most files are already compressed.	None

Software compression makes heavy demands on the router's processor. The maximum compressed serial line rate depends on the type of Cisco router you are using and which compression algorithm you specify. Table 2 shows a summary of the compressed serial line rates for software compression. The maximums shown in Table 2 apply to the "combined" serial compressed load on the router. For example, a Cisco 4000 series router could handle four 64-kbps lines using Stacker or one 256-kbps line. These maximums also assume there is very little processor load on the router aside from compression. Lower these numbers when the router is required to do other processor-intensive tasks.

Table 2 Combined Compressed Serial Line Rates (Software Compression)

Router Family	Cisco 1000	Cisco 3000	Cisco 4000	Cisco 4500	Cisco 4700	Cisco 7000
Stacker (kbps)	128	128	256	500	T1	256
Predictor (kbps)	256	256	500	T1	2xT1	500

Cisco recommends that you do not adjust the maximum transmission unit (MTU) for the serial interface and the LAPB maximum bits per frame (N1) parameter.

Examples

The following example enables hardware compression and PPP encapsulation on serial interface 3/1/0.

```
interface serial 3/1/0
 encapsulate ppp
 compress stac
```

The following example enables predictor compression on serial interface 0 for a LAPB link:

```
interface serial 0
 encapsulation lapb
 compress predictor
```

Related Commands

A dagger (†) indicates that the command is documented outside of this chapter.

encapsulation lapb
encapsulation ppp †
encapsulation x25
show compress
show processes †

fddi full-duplex

To enable full-duplex mode on the FDDI full-duplex, single-mode port adapter (PA-F/FD-SM) and FDDI full-duplex, multimode port adapter (PA-F/FD-MM) on the Cisco 7000 series routers with RSP7000 and Cisco 7500 series routers, use the **fddi full-duplex** interface configuration command. FDDI full-duplex allows an FDDI ring with exactly two stations to transform the ring into a full-duplex, point-to-point topology. Use the **no** form of this command to disable this feature.

fddi full-duplex
no fddi full-duplex

Syntax Description

This command has no arguments or keywords.

Default

Half-duplex mode

Command Mode

Interface configuration

Usage Guidelines

In order to operate in full-duplex mode, there must be only two stations on the ring, the two stations must be capable of operating in full-duplex mode, and both stations must complete a full-duplex autoconfiguration protocol. There is no FDDI token in full-duplex mode.

Full-duplex autoconfiguration protocol allows a station to dynamically and automatically operate in either half-duplex (or ring) or full-duplex mode, and ensures that the stations fall back to ring mode when a configuration change occurs, such as a third station joining the ring.

After booting up, the stations begin operation in ring mode. While the station performs the full-duplex autoconfiguration protocol, the station continues to provide data link services to its users. Under normal conditions, the transition between half-duplex mode and full-duplex mode is transparent to the data-link users. The data-link services provided by full-duplex mode are functionally the same as the services provided by half-duplex mode.

Use this command if your equipment on the other end is capable of full-duplex mode.

If you change the full-duplex configuration (for example from disabled to enabled) on supported interfaces, the interface resets.

If the interface does not support full-duplex, the following message is displayed, and no changes are made to the interface. To determine whether the interface supports full-duplex, use the **show interfaces fddi** command.

```
%FDDI-3-FDDIFAIL: Interface Fddi0/0/0, doesn’t support, fddi full = 0x0
```

Example

The following example enables full-duplex mode on FDDI interface 0:

```
interface fddi 0/1/0
 fddi full-duplex
```

Related Commands

interface fddi
show interfaces fddi

invert data

To invert the data stream, use the **invert data** interface configuration command. This command applies only to the Cisco 7000 series routers with RSP7000, Cisco 7200 series routers, and Cisco 7500 series routers. Use the **no** form of this command to disable this feature.

invert data
no invert data

Syntax Description

This command has no arguments or keywords.

Default

Data in not inverted

Command Mode

Interface configuration

Usage Guidelines

If the interface on the PA-8T synchronous serial port adapter is used to drive a dedicated T1 line that does not have B8ZS encoding (a method to avoid 15 zeros), the data stream must be inverted (both TXD and RXD) either in the connecting CSU/DSU or the interface.

By inverting the HDLC data stream, the HDLC zero insertion algorithm becomes a ones insertion algorithm that satisfies the T1 requirements. Be careful not to invert data both on the interface and on the CSU/DSU as two data inversions will cancel each other out.

Example

The following example inverts data on serial interface 3/1/0:

```
interface serial 3/1/0
 invert data
```

invert txclock

To invert the transmit clock signal, use the **invert txclock** interface configuration command. This command applies only to the Cisco 7000 series, Cisco 7200 series, and Cisco 7500 series routers. To return to the transmit clock signal to its initial state, use the **no** form of this command.

invert txclock
no invert txclock

Syntax Description

This command has no arguments or keywords.

Default

Transmit clock signal is not inverted

Command Mode

Interface configuration

Usage Guidelines

Systems that use long cables or cables that are not transmitting the TxC signal (transmit echoed clock line, also known as TXCE or SCTE.clock) may experience high error rates when operating at the higher transmission speeds. For example, if a PA-8T synchronous serial port adapter is reporting a high number of error packets, a phase shift might be the problem. Inverting the clock may correct this shift.

When a PA-8T port adapter interface is DTE, the **invert txclock** command inverts the TxC signal it received from the remote DCE. When the PA-8T port adapter interface is DCE, this command changes the signal beck to its original phase.

Example

In the following example, the clock signal on serial interface 3/0 is inverted:

```
interface serial 3/0
 invert txclock
```

nrzi-encoding

To enable nonreturn-to-zero inverted (NRZI) line-coding format, use the **nrzi-encoding** interface configuration command. Use the **no** form of this command to disable this capability.

nrzi-encoding
no nrzi-encoding

nrzi-encoding [**mark**] (Cisco 7000 series routers with RSP7000, Cisco 7200 series routers, and Cisco 7500 series routers)

Syntax Description

mark	(Optional) Specifies that NRZI mark encoding is required on the PA-8T synchronous serial port adapter on the Cisco 7000 series routers with RSP7000, Cisco 7200 series routers, and Cisco 7500 series routers. If mark is not specified, NRZI space encoding is used.

Default

Disabled

Command Mode

Interface configuration

Usage Guidelines

All FSIP and PA-8T interface types support nonreturn-to-zero (NRZ) and nonreturn-to-zero inverted (NRZI) format. This is a line-coding format that is required for serial connections in some environments. NRZ encoding is most common. NRZI encoding is used primarily with EIA/TIA-232 connections in IBM environments.

Examples

In the following example, serial interface 1 is configured for NRZI encoding:

```
interface serial 1
 nrzi-encoding
```

In the following example, serial interface 3/1/0 is configured for NRZI mark encoding:

```
interface serial 3/1/0
 nrzi-encoding mark
```

show compress

To display compression statistics, use the **show compress** EXEC command.

show compress

Syntax Description

This command has no arguments or keywords.

Command Mode

EXEC

Sample Displays

The following is sample output from the **show compress** command when software compression is used on the router:

```
Router# show compress

Serial0
uncompressed bytes xmt/rcv 10710562/11376835
1  min avg ratio xmt/rcv 2.773/2.474
5  min avg ratio xmt/rcv 4.084/3.793
10 min avg ratio xmt/rcv 4.125/3.873
no bufs xmt 0 no bufs rcv 0
resets 0
```

Table 3 describes the fields shown in the display.

Table 3 Show Compress Field Descriptions—Software Compression

Field	Description
Serial0	Name and number of the interface.
uncompressed bytes xmt/rcv	Total number of uncompressed bytes sent and received.
1 min avg ratio xmt/rcv 5 min avg ratio xmt/rcv 10 min avg ratio xmt/rcv	Static compression ratio for bytes sent and received, averaged over 1, 5, and 10 minutes.
no bufs xmt	Number of times buffers were not available to compress data being sent.
no bufs rcv	Number of times buffers were not available to uncompress data being received.
resets	Number of resets (for example, line errors could cause resets).

The following is sample output from the **show compress** command when hardware compression is enabled (that is, compression is implemented in the CSA hardware):

```
Router# show compress

Serial6/1
     Hardware compression enabled
     Compressed bytes sent:     402 bytes     0 Kbits/sec    ratio: 4.092
     Compressed bytes recv:     390 bytes     0 Kbits/sec    ratio: 3.476
     restarts:1
     last clearing of counters: 1278 seconds
```

Table 4 describes the fields shown in the display. The information displayed by the **show compress** command is the same for hardware and distributed compression.

Table 4 Show Compress Field Descriptions—Hardware or Distributed Compression

Field	Description
Serial6/1	Name and number of the interface.
Compressed bytes sent	Total number of compressed bytes sent including the kilobits per second.
Compressed bytes recv	Total number of compressed bytes received including the kilobits per second.
ratio	Compression ratio for bytes sent and received since the link last came up or since the counters were last cleared.
restarts	Number of times the compression process restarted or reset.
last clearing of counters	Duration since the last time the counters were cleared with the **clear counters** command.

Related Command

compress

show interfaces fddi

Use the **show interfaces fddi** EXEC command to display information about the FDDI interface.

show interfaces fddi *number* [**accounting**]
show interfaces fddi [*slot*/*port-adapter*/*port*] [**accounting**] (for ports on VIP2 cards in the Cisco 7000 series and the Cisco 7500 series routers)

Syntax Description

number	Port number on the selected interface.
accounting	(Optional) Displays the number of packets of each protocol type that have been sent through the interface.
slot	(Optional) On the Cisco 7000 series and 7500 series, slot location of the interface processor.
port-adapter	(Optional) On the Cisco 7000 series and 7500 series, specifies the ports on a VIP2 card. The value can be 0 or 1.
port	(Optional) On the Cisco 7000 series and 7500 series, port number on interface.

Command Mode

EXEC

Sample Displays

The following is a sample partial display of FDDI-specific data from the **show interfaces fddi** command on a Cisco 7000:

```
Router> show interfaces fddi 3/0

Fddi3/0 is up, line protocol is up
  Hardware is cxBus Fddi, address is 0000.0c02.adf1 (bia 0000.0c02.adf1)
  Internet address is 131.108.33.14, subnet mask is 255.255.255.0
  MTU 4470 bytes, BW 100000 Kbit, DLY 100 usec, rely 255/255, load 1/255
  Encapsulation SNAP, loopback not set, keepalive not set
  ARP type: SNAP, ARP Timeout 4:00:00
  Phy-A state is  active, neighbor is   B, cmt signal bits 008/20C, status ILS
  Phy-B state is  active, neighbor is   A, cmt signal bits 20C/008, status ILS
  ECM is in, CFM is thru, RMT is ring_op
  Token rotation 5000 usec, ring operational 21:32:34
  Upstream neighbor 0000.0c02.ba83, downstream neighbor 0000.0c02.ba83
  Last input 0:00:05, output 0:00:00, output hang never
  Last clearing of “show interface” counters 0:59:10
  Output queue 0/40, 0 drops; input queue 0/75, 0 drops
  Five minute input rate 69000 bits/sec, 44 packets/sec
  Five minute output rate 0 bits/sec, 1 packets/sec
     113157 packets input, 21622582 bytes, 0 no buffer
     Received 276 broadcasts, 0 runts, 0 giants
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
     4740 packets output, 487346 bytes, 0 underruns
     0 output errors, 0 collisions, 0 interface resets, 0 restarts
     0 transitions, 2 traces, 3 claims, 2 beacons
```

The following is a sample display of the **show interfaces fddi** command for the full-duplex FDDI port adapter on a Cisco 7500:

```
Router# show interfaces fddi 0/1/0
Fddi0/1/0 is up, line protocol is up
  Hardware is cxBus FDDI, address is 0060.3e33.3608 (bia 0060.3e33.3608)
  Internet address is 2.1.1.1/24
  MTU 4470 bytes, BW 100000 Kbit, DLY 100 usec, rely 255/255, load 1/255
  Encapsulation SNAP, loopback not set, keepalive not set
  ARP type: SNAP, ARP Timeout 04:00:00
  FDX supported, FDX enabled, FDX state is operation
  Phy-A state is maintenance, neighbor is Unknown, status HLS
  Phy-B state is active, neighbor is A, status SILS
  ECM is in, CFM is c_wrap_b, RMT is ring_op,
  Requested token rotation 5000 usec, negotiated 4997 usec
  Configured tvx is 2500 usec
  LER for PortA = 0A, LER for PortB = 0A ring operational 00:02:45
  Upstream neighbor 0060.3e73.4600, downstream neighbor 0060.3e73.4600
  Last input 00:00:12, output 00:00:13, output hang never
  Last clearing of “show interface” counters never
  Queueing strategy: fifo
  Output queue 0/40, 0 drops; input queue 0/75, 0 drops
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     62 packets input, 6024 bytes, 0 no buffer
     Received 18 broadcasts, 0 runts, 0 giants
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
     71 packets output, 4961 bytes, 0 underruns
     0 output errors, 0 collisions, 0 interface resets
     0 output buffer failures, 0 output buffers swapped out
     3 transitions, 0 traces,  100 claims, 0 beacon
```

Table 5 describes the **show interfaces fddi** display fields.

Table 5 Show Interfaces FDDI Field Descriptions

Field	Description
Fddi is {up | down}...is administratively down	Gives the interface processor unit number and tells whether the interface hardware is currently active and can transmit and receive or if it has been taken down by an administrator.
line protocol is {up | down}	Indicates whether the software processes that handle the line protocol consider the interface usable.
Hardware	Provides the hardware type, followed by the hardware address.
Internet address	IP address, followed by subnet mask.
MTU	Maximum Transmission Unit of the interface.
BW	Bandwidth of the interface in kilobits per second.
DLY	Delay of the interface in microseconds.
rely	Reliability of the interface as a fraction of 255 (255/255 is 100% reliability), calculated as an exponential average over 5 minutes.
load	Load on the interface as a fraction of 255 (255/255 is completely saturated), calculated as an exponential average over 5 minutes.
Encapsulation	Encapsulation method assigned to interface.
loopback	Indicates whether or not loopback is set.
keepalive	Indicates whether or not keepalives are set.

Table 5 Show Interfaces FDDI Field Descriptions (Continued)

ARP type	Type of Address Resolution Protocol assigned.
FDX	Displays full-duplex information. Values are: not supported or supported. When the value is supported, the display indicates whether full-duplex is enabled or disabled. When enabled, the state of the FDX negotiation process is displayed. The negotiation states only relate to the full-duplex negotiation process. You must also ensure that the interface is up and working by looking at other fields in the **show interfaces fddi** command such as line protocol and RMT. Negotiation states are: • idle—interface is working but not in full-duplex mode yet. If persistent, it could mean that the interface did not meet all negotiations conditions (for example, there are more than two stations in the ring). • request—interface is working but not in full-duplex mode yet. If persistent, it could mean that the remote interface does not support full-duplex or full-duplex is not enabled on the interface. • confirm—transient state. • operation—negotiations completed successfully, and both stations are operating in full-duplex mode.
Phy-{A | B}	Lists the state the Physical A or Physical B connection is in; one of the following: off, active, trace, connect, next, signal, join, verify, or break.
neighbor	State of the neighbor: • A—Indicates that the connection management (CMT) process has established a connection with its neighbor. The bits received during the CMT signaling process indicate that the neighbor is a Physical A type dual attachment station (DAS) or concentrator that attaches to the primary ring IN and the secondary ring OUT when attaching to the dual ring. • S—Indicates that the CMT process has established a connection with its neighbor and that the bits received during the CMT signaling process indicate that the neighbor is one Physical type in a single attachment station (SAS). • B—Indicates that the CMT process has established a connection with its neighbor and that the bits received during the CMT signaling process indicate that the neighbor is a Physical B dual attachment station or concentrator that attaches to the secondary ring IN and the primary ring OUT when attaching to the dual ring. • M—Indicates that the CMT process has established a connection with its neighbor and that the bits received during the CMT signaling process indicate that the router's neighbor is a Physical M-type concentrator serving as a Master to a connected station or concentrator. • unk—Indicates that the network server has not completed the CMT process and, as a result, does not know about its neighbor. See the section "Setting Bit Control" for an explanation of the bit patterns.
cmt signal bits	Shows the transmitted/received CMT bits. The transmitted bits are 0x008 for a Physical A type and 0x20C for Physical B type. The number after the slash (/) is the received signal bits. If the connection is not active, the received bits are zero (0); see the line beginning Phy-B in the display.

Table 5 Show Interfaces FDDI Field Descriptions (Continued)

status	Status value displayed is the actual status on the fiber. The FDDI standard defines the following values: • LSU—Line State Unknown, the criteria for entering or remaining in any other line state have not been met. • NLS—Noise Line State is entered upon the occurrence of 16 potential noise events without satisfying the criteria for entry into another line state. • MLS—Master Line State is entered upon the receipt of eight or nine consecutive HQ or QH symbol pairs. • ILS—Idle Line State is entered upon receipt of four or five idle symbols. • HLS—Halt Line State is entered upon the receipt of 16 or 17 consecutive H symbols. • QLS—Quiet Line State is entered upon the receipt of 16 or 17 consecutive Q symbols or when carrier detect goes low. • ALS—Active Line State is entered upon receipt of a JK symbol pair when carrier detect is high. • OVUF—Elasticity buffer Overflow/Underflow. The normal states for a connected Physical type are ILS or ALS. If the report displays the QLS status, this indicates that the fiber is disconnected from Physical B, or that it is not connected to another Physical type, or that the other station is not running.
ECM is...	ECM is the SMT entity coordination management, which overlooks the operation of CFM and PCM. The ECM state can be one of the following: • out—The router is isolated from the network. • in—The router is actively connected to the network. This is the normal state for a connected router. • trace—The router is trying to localize a stuck beacon condition. • leave—The router is allowing time for all the connections to break before leaving the network. • path_test—The router is testing its internal paths. • insert—The router is allowing time for the optical bypass to insert. • check—The router is making sure optical bypasses switched correctly. • deinsert—The router is allowing time for the optical bypass to deinsert.

Table 5 Show Interfaces FDDI Field Descriptions (Continued)

CFM is...	Contains information about the current state of the MAC connection. The Configuration Management state can be one of the following: • isolated—The MAC is not attached to any Physical type. • wrap_a—The MAC is attached to Physical A. Data is received on Physical A and transmitted on Physical A. • wrap b—The MAC is attached to Physical B. Data is received on Physical B and transmitted on Physical B. • wrap_s—The MAC is attached to Physical S. Data is received on Physical S and transmitted on Physical S. This is the normal mode for a single attachment station (SAS). • thru—The MAC is attached to Physical A and B. Data is received on Physical A and transmitted on Physical B. This is the normal mode for a dual attachment station (DAS) with one MAC. The ring has been operational for 1 minute and 42 seconds.
RMT is...	RMT (Ring Management) is the SMT MAC-related state machine. The RMT state can be one of the following: • isolated—The MAC is not trying to participate in the ring. This is the initial state. • non_op—The MAC is participating in ring recovery, and ring is not operational. • ring_op—The MAC is participating in an operational ring. This is the normal state while the MAC is connected to the ring. • detect—The ring has been nonoperational for longer than normal. Duplicate address conditions are being checked. • non_op_dup—Indications have been received that the address of the MAC is a duplicate of another MAC on the ring. Ring is not operational. • ring_op_dup—Indications have been received that the address of the MAC is a duplicate of another MAC on the ring. Ring is operational in this state. • directed—The MAC is sending beacon frames notifying the ring of the stuck condition. • trace—Trace has been initiated by this MAC, and the RMT state machine is waiting for its completion before starting an internal path test.
token rotation	Token rotation value is the default or configured rotation value as determined by the **fddi token-rotation-time** command. This value is used by all stations on the ring. The default is 5000 microseconds.
negotiated	Actual (negotiated) target token rotation time.
ring operational	When the ring is operational, the displayed value will be the negotiated token rotation time of all stations on the ring. Operational times are displayed by the number of hours:minutes:seconds the ring has been up. If the ring is not operational, the message “ring not operational” is displayed.
Configured tvx	Transmission timer.
LER	Link error rate.

Table 5 Show Interfaces FDDI Field Descriptions (Continued)

Upstream | downstream neighbor	Displays the canonical MAC address of outgoing upstream and downstream neighbors. If the address is unknown, the value will be the FDDI unknown address (0x00 00 f8 00 00 00).
Last input	Number of hours, minutes, and seconds since the last packet was successfully received by an interface. Useful for knowing when a dead interface failed.
output	Number of hours, minutes, and seconds since the last packet was successfully transmitted by an interface.
output hang	Number of hours, minutes, and seconds (or never) since the interface was last reset because of a transmission that took too long. When the number of hours in any of the "last" fields exceeds 24 hours, the number of days and hours is printed. If that field overflows, asterisks are printed.
Last clearing	Time at which the counters that measure cumulative statistics (such as number of bytes transmitted and received) shown in this report were last reset to zero. Note that variables that might affect routing (for example, load and reliability) are not cleared when the counters are cleared. *** indicates the elapsed time is too large to be displayed. 0:00:00 indicates the counters were cleared more than 2^{31}ms (and less than 2^{32}ms) ago.
Queueing strategy	First-in, first-out queuing strategy (other queueing strategies you might see are priority-list, custom-list, and weighted fair).
Output queue, input queue, drops	Number of packets in output and input queues. Each number is followed by a slash, the maximum size of the queue, and the number of packets dropped due to a full queue.
Five-minute input rate Five-minute output rate	Average number of bits and packets transmitted per second in the last 5 minutes. The five-minute input and output rates should be used only as an approximation of traffic per second during a given 5-minute period. These rates are exponentially weighted averages with a time constant of 5 minutes. A period of four time constants must pass before the average will be within two percent of the instantaneous rate of a uniform stream of traffic over that period.
packets input	Total number of error-free packets received by the system.
bytes	Total number of bytes, including data and MAC encapsulation, in the error free packets received by the system.
no buffer	Number of received packets discarded because there was no buffer space in the main system. Compare with ignored count. Broadcast storms on Ethernets and bursts of noise on serial lines are often responsible for no input buffer events.
broadcasts	Total number of broadcast or multicast packets received by the interface.
runts	Number of packets that are discarded because they are smaller than the medium's minimum packet size.
giants	Number of packets that are discarded because they exceed the medium's maximum packet size.

Table 5 Show Interfaces FDDI Field Descriptions (Continued)

CRC	Cyclic redundancy checksum generated by the originating LAN station or far-end device does not match the checksum calculated from the data received. On a LAN, this usually indicates noise or transmission problems on the LAN interface or the LAN bus itself. A high number of CRCs is usually the result of collisions or a station transmitting bad data.
frame	Number of packets received incorrectly that have a CRC error and a noninteger number of octets. On a LAN, this is usually the result of collisions or a malfunctioning Ethernet device. On an FDDI LAN, this also may be the result of a failing fiber (cracks) or a hardware malfunction.
overrun	Number of times the serial receiver hardware was unable to hand received data to a hardware buffer because the input rate exceeded the receiver's ability to handle the data.
ignored	Number of received packets ignored by the interface because the interface hardware ran low on internal buffers. These buffers are different from the system buffers mentioned previously in the buffer description. Broadcast storms and bursts of noise can cause the ignored count to be increased.
packets output	Total number of messages transmitted by the system.
bytes	Total number of bytes, including data and MAC encapsulation, transmitted by the system.
underruns	Number of transmit aborts (when the router cannot feed the transmitter fast enough).
output errors	Sum of all errors that prevented the final transmission of datagrams out of the interface being examined. Note that this may not balance with the sum of the enumerated output errors, because some datagrams may have more than one error, and others may have errors that do not fall into any of the specifically tabulated categories.
collisions	Because an FDDI ring cannot have collisions, this statistic is always zero.
interface resets	Number of times an interface has been reset. The interface may be reset by the administrator or automatically when an internal error occurs.
restarts	Should always be zero for FDDI interfaces.
output buffer failures	Number of no resource errors received on the output.
output buffers swapped out	Number of packets swapped to DRAM.
transitions	The number of times the ring made a transition from ring operational to ring nonoperational, or vice versa. A large number of transitions indicates a problem with the ring or the interface.
traces	Trace count applies to both the FCI, FCIT, and FIP. Indicates the number of times this interface started a trace.
claims	Pertains to FCIT and FIP only. Indicates the number of times this interface has been in claim state.
beacons	Pertains to FCIT and FIP only. Indicates the number of times the interface has been in beacon state.

The following is an example that includes the **accounting** option. When you use the **accounting** option, only the accounting statistics are displayed.

```
Router> show interfaces fddi 3/0 accounting

Fddi3/0
       Protocol    Pkts In   Chars In   Pkts Out  Chars Out
             IP       7344    4787842       1803    1535774
      Appletalk      33345    4797459      12781    1089695
        DEC MOP          0          0        127       9779
            ARP          7        420         39       2340
```

Table 6 describes the **show interfaces fddi** display fields.

Table 6 Show Interfaces FDDI Field Descriptions—Accounting

Field	Description
Protocol	Protocol that is operating on the interface.
Pkts In	Number of packets received for that protocol.
Chars In	Number of characters received for that protocol.
Pkts Out	Number of packets transmitted for that protocol.
Chars Out	Number of characters transmitted for that protocol.

Cisco Connection Online

Cisco Connection Online (CCO), formerly Cisco Information Online (CIO), is Cisco Systems' primary, real-time support channel. Maintenance customers and partners can self-register on CCO to obtain additional content and services.

Available 24 hours a day, 7 days a week, CCO provides a wealth of standard and value-added services to Cisco's customers and business partners. CCO services include product information, software updates, release notes, technical tips, the Bug Navigator, configuration notes, brochures, descriptions of service offerings, and download access to public and authorized files.

CCO serves a wide variety of users through two interfaces that are updated and enhanced simultaneously—a character-based version and a multimedia version that resides on the World Wide Web (WWW). The character-based CCO supports Zmodem, Kermit, Xmodem, FTP, and Internet e-mail, and is excellent for quick access to information over lower bandwidths. The WWW version of CCO provides richly formatted documents with photographs, figures, graphics, and video, as well as hyperlinks to related information.

You can access CCO in the following ways:

- WWW: http://www.cisco.com.
- WWW: http://www-europe.cisco.com.
- WWW: http://www-china.cisco.com.
- Telnet: cco.cisco.com.
- Modem: From North America, 408 526-8070; from Europe, 33 1 64 46 40 82. Use the following terminal settings: VT100 emulation; databits: 8; parity: none; stop bits: 1; and baud rates up to 14.4 kbps.

For a copy of CCO's Frequently Asked Questions (FAQ), contact cco-help@cisco.com. For additional information, contact cco-team@cisco.com.

Note If you are a network administrator and need personal technical assistance with a Cisco product that is under warranty or covered by a maintenance contract, contact Cisco's Technical Assistance Center (TAC) at 800 553-2447, 408 526-7209, or tac@cisco.com. To obtain general information about Cisco Systems, Cisco products, or upgrades, contact 800 553-6387, 408 526-7208, or cs-rep@cisco.com.

Cisco Connection Documentation

The complete caveats against this release are available on the Cisco Connection Documentation, Enterprise Series CD—formerly UniverCD—which is the Cisco library of product information on CD-ROM. On the CD, access the Cisco IOS 11.1 caveats in the Cisco IOS Release 11.1 database.

The CD is updated and shipped monthly so it might be more current than printed documentation. To order the Cisco Connection Documentation, Enterprise Series CD, contact your local sales representative or call Customer Service. The CD is available both as a single CD and as an annual subscription.You can also access Cisco technical documentation on the World Wide Web URL http://www.cisco.com.

This document is to be used in conjunction with the *Release Notes for Cisco IOS Release 11.1* and the Cisco IOS Release 11.1 *Configuration Fundamentals Configuration Guide* and *Configuration Fundamentals Command Reference*.

969R