CISCO SYSTEMS

Doc. No. 78-1062-05

FDDI Interface Processor (FIP) Installation and Configuration

Product Numbers: CX-FIP-MM=, CX-FIP-SS=, CX-FIP-MS=, CX-FIP-SM=, and CAB-FMDD=

This document provides instructions for installing and upgrading the Fiber Distributed Data Interface (FDDI) Interface Processor (FIP) in a Cisco 7000 series and Cisco 7500 series router. The upgrade instructions include steps for upgrading the FIP microcode by downloading a new image. This document also contains basic configuration steps and examples for configuring the FDDI interfaces on a new FIP.

For complete descriptions of interface subcommands and the configuration options available for FDDI interfaces, refer to the *Router Products Command Summary* and *Router Products Command Reference* publications, which are available on UniverCD, Cisco's online library of product documentation, or in print.

Sections in this document include the following:

Product Description

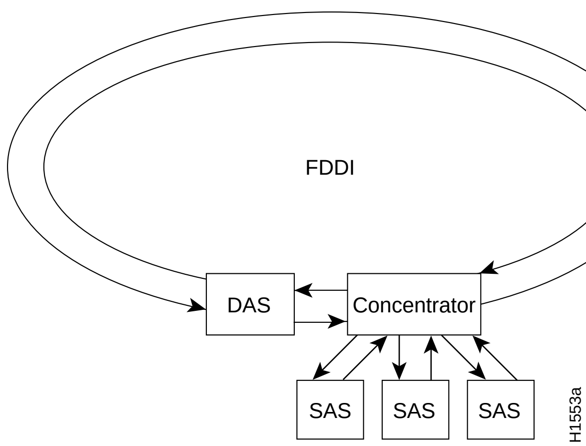
This section provides an overview of FDDI, a description of the FIP, and brief descriptions of the Cisco 7000 series and the Cisco 7500 series routers. For a complete system description, refer to the hardware installation and maintenance publication appropriate to your chassis type.

FDDI Overview

FDDI, which specifies a 100-Mbps, token-passing dual-ring network using fiber optic transmission media, is defined by the ANSI X3.1 standard and by ISO 9314, the international version of the ANSI standard. An FDDI network comprises two token-passing fiber optic rings: a primary ring and a secondary ring.

A ring consists of two or more point-to-point connections between adjacent stations. On most networks, the primary ring is used for data communication, and the secondary ring is used as a backup. Class B, or single attachment stations (SASs), attach to one ring and are typically attached through a concentrator; Class A, or dual attachment stations (DASs), attach to both rings. Figure 1 shows a typical FDDI configuration with both DAS and SAS connections.

Figure 1 Typical FDDI Configuration with DAS, Concentrator, and SAS



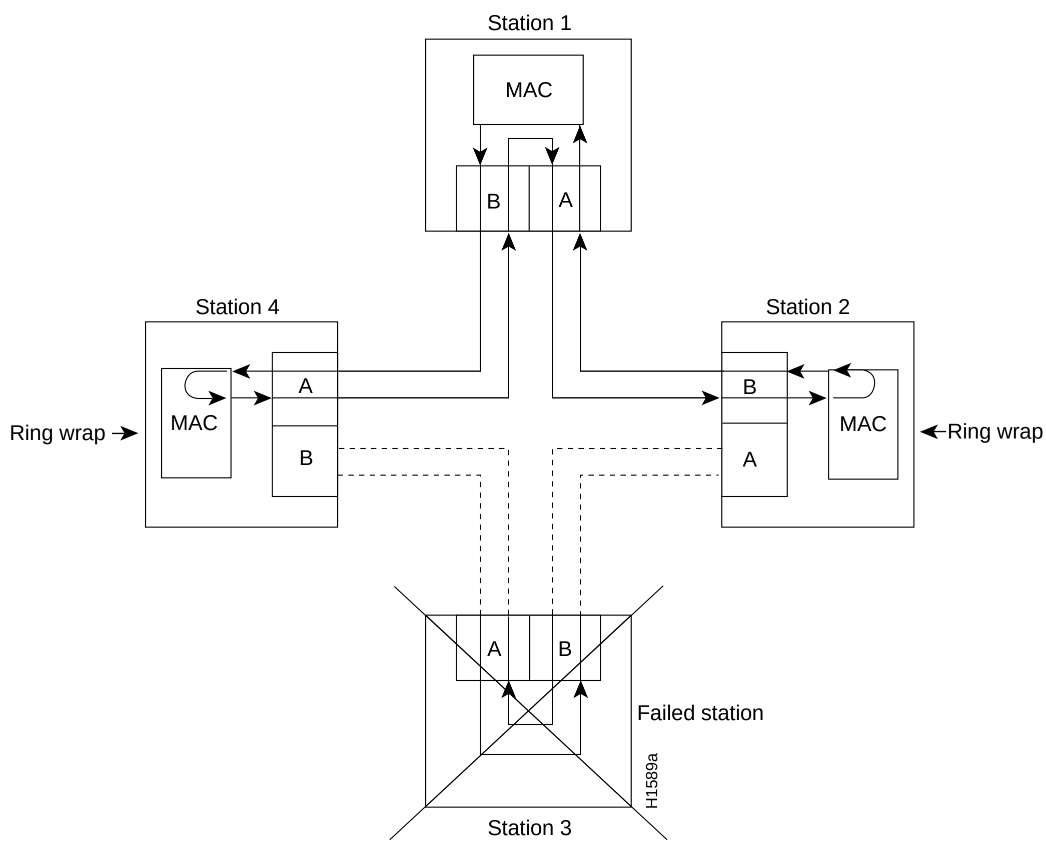
SASs (Class B) typically attach to the primary ring through a concentrator, which provides connections for multiple SASs. The concentrator ensures that a failure or power down of any SAS does not interrupt the ring. SASs use one transmit port and one receive port to attach to the single ring. DASs (Class A) have two physical ports, designated PHY A and PHY B, each of which connects the station to both the primary and secondary rings. Each port is a receiver for one ring and a transmitter for the other. For example, PHY A receives traffic from the primary ring and PHY B transmits to it.

The dual rings in an FDDI network provide fault tolerance. If a station on a dual ring shuts down or fails, such as Station 3 in Figure 2, the ring automatically wraps (doubles back on itself) to form a single contiguous ring. This removes the failed station from the ring, but allows the other stations to continue operation. In Figure 2, the ring wraps to eliminate Station 3 and forms a smaller ring that includes only Stations 1, 2, and 4. A second failure could cause the ring to wrap in both directions from the point of failure, which would segment the ring into two separate rings that could not communicate with each other.

For example, if Station 1 in Figure 2 fails after Station 3 fails, Stations 2 and 4 will each be isolated because no path for communication exists between them. Subsequent failures cause additional segmentation. Optical bypass switches avoid segmentation by eliminating failed stations from the ring.

An optical bypass switch allows the light signal to pass directly through it, completely bypassing the failed or shut down station. If an optical bypass switch had been installed at Station 3 in the example ring in Figure 2, it would have allowed the light signal to pass through the switch and maintain its existing path and direction without wrapping back on itself.

Figure 2 DAS Station Failure and Ring Recovery Example



Another technique for fault tolerance is dual homing, whereby critical devices are attached to two concentrators. Only the designated primary concentrator is active unless it (or its link) fails. If the primary does fail, the backup (passive) concentrator is automatically activated and sustains the ring.

FDDI uses two types of fiber optic cable: single-mode (also called monomode) and multimode. *Mode* refers to the angle at which light rays (signals) are reflected and propagated through the optical fiber core, which acts as a waveguide for the light signals. Multimode fiber has a relatively thick core (62.5/125-micron) that reflects light rays at many angles. Single-mode fiber has a narrow core (8.7 to 10/125-micron) that allows the light to enter only at a single angle. Although multimode fiber allows more light signals to enter at a greater variety of angles (modes), the different angles create multiple propagation paths that cause the signals to spread out in time and limits the rate at which data can be accurately received. This distortion does not occur on the single path of the single-mode signal; therefore, single-mode fiber is capable of higher bandwidth and greater cable run distances that multimode fiber. In addition, multimode transmitters usually use LEDs as a light source, and single-mode transmitters use a laser diode, which is capable of sustaining faster data rates. Both types use a photodiode detector at the receiver to translate the light signal into electrical signals.

The FDDI standard sets total fiber lengths of 2 kilometers (1.2 miles) for multimode fiber and 10 kilometers (6.2 miles) for single-mode fiber. (The maximum circumference of the FDDI network is only half the specified distance because of signal wrapping or loopback that occurs during fault correction.) The standard allows a maximum of 500 stations with a maximum distance between active stations of 2 kilometers.

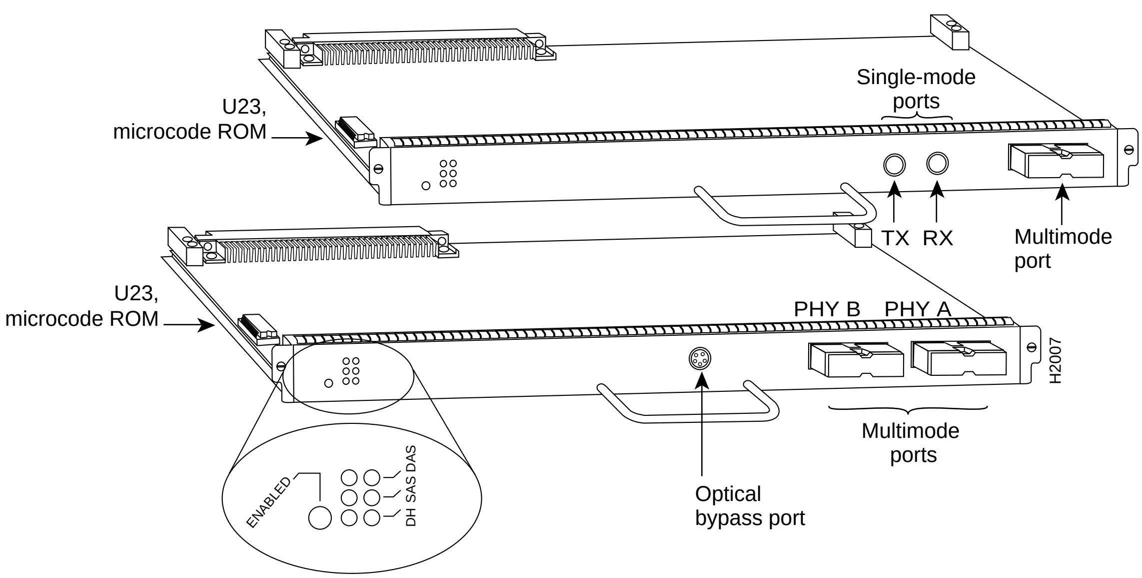
The FIP supports both Class A and Class B station connections and provides an interface for both single-mode and multimode fiber-optic cable. The two physical ports (PHY A and PHY B) are available with either single-mode (FC) or multimode, media interface connector (MICs), or with a combination of one of each for matching multimode and single-mode fiber in the same FDDI network.

The FIP FDDI implementation complies with Version 6.1 of the X3T9.5 FDDI specification, offering a Class A dual attachment interface that supports the fault-recovery methods of DAS. The FIP supports dual homing and optical bypass and complies with ANSI X3.1 and ISO 9314 FDDI standards.

FIP Description

The FIP contains a 16-million-instructions-per-second (mips) processor for high-speed (100-Mbps) interface rates and the industry-standard, AMD SuperNet chipset for interoperability. Figure 3 shows a multimode/multimode FIP on the bottom (CX-FIP-MM) and a single-mode/multimode FIP on the top (CX-FIP-SM). The FIP supports optical bypass on the CX-FIP-MM and CX-FIP-SS models. The default FIP microcode resides on a ROM in socket U23. (See Figure 3.)

Figure 3 FIP, CX-FIP-MM (Bottom) and CX-FIP-SM (Top)



Note The CX-FIP-SS model also has the optical bypass port, which is shown on the CX-FIP-MM model in Figure 3.

Each FIP provides a single network interface for both multimode and single-mode FDDI networks. The two FIP connectors are available in any combination of multimode (MIC) or single-mode (FC) connectors for matching multimode and single-mode fiber in the same FDDI network.

The following combinations are available:

- CX-FIP-MM—FDDI PHY-A multimode, PHY-B multimode interface processor with optical bypass switch capability
- CX-FIP-MS—FDDI PHY-A multimode, PHY-B single-mode interface processor
- CX-FIP-SM—FDDI PHY-A single-mode, PHY-B multimode interface processor
- CX-FIP-SS—FDDI PHY-A single-mode, PHY-B single-mode interface processor with optical bypass switch capability

Each FIP provides the interface for connection to a Class A DAS (with primary and secondary rings), or to a Class B SAS (with only a primary ring). The multimode or single-mode ports on the FIP provide a direct connection to the external FDDI network.

A six-pin mini-DIN connector on the multimode-multimode FIP (CX-FIP-MM) and the single-mode/single-mode FIP (CX-FIP-SS) provides the connection for an optical bypass switch. When the interface is shut down, the bypass switch allows the light signal to pass directly from the receive port to the transmit port on the bypass switch, completely *bypassing* the FIP transceivers. The bypass switch does not repeat the signal, and significant signal loss may occur when transmitting to stations at maximum distances. Optical bypass switches typically use a six-pin DIN or mini-DIN connector. A DIN-to-mini-DIN adapter cable is included with the CX-FIP-MM to allow connection to either type of connector. For a detailed description of optical bypass switch connections, refer to the section “Installing an Optical Bypass Switch” on page 26.

FIP Microcode

The FIP microcode (firmware) is a software image that provides card-specific software instructions and support for Connection Management (CMT) functions. A ROM in socket U23 contains the default FIP microcode.

The Cisco 7000 and Cisco 7500 series support downloadable microcode, which enables you to upgrade microcode versions by downloading new microcode images, storing them in Flash memory, and instructing the system to load an image from Flash instead of the default ROM image. You can store multiple images for an interface type, and with a configuration command you can instruct the system to load any one of them or the default ROM image. All interfaces of the same type (FIP, HIP, and so on) will load the same microcode image, either from the default ROM image or from a single image stored in Flash.

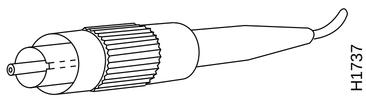
Although multiple microcode versions for a specific interface type can be stored concurrently in Flash, only one image can load at startup. The **show controller cxbus** command displays the currently loaded and running microcode version for each interface processor. The **show configuration** EXEC command shows the current system instructions for loading microcode at startup.

For a complete description of microcode and downloading procedures, refer to the section “Upgrading Microcode” on page 35.

FDDI Transceivers and Connectors

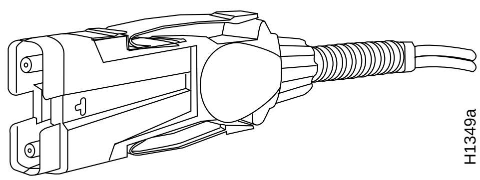
The single-mode interface uses simplex FC-type connectors (see Figure 4) for the transmit and receive ports. The connector accepts standard 8.7 to 10/125-micron, single-mode fiber-optic cable.

Figure 4 Single-Mode FDDI Network Interface Connectors, FC Type



The multimode connector is an FDDI-standard physical sublayer (PHY) connector that encodes and decodes the data into a format acceptable for fiber transmission. The multimode connector accepts standard 62.5/125-micron, multimode fiber-optic cable using the media interface cable (MIC) and, with proper cable terminators, can accept 50/125 micron fiber-optic cable. Multimode uses the integrated MIC shown in Figure 5, at both the FIP and network end.

Figure 5 Multimode FDDI Network Interface Connector, MIC Type



The single-mode/single-mode FIP (CX-FIP-SS) and multimode/multimode FIP (CX-FIP-MM) each provide a control port for an optical bypass switch, which allows the light signal to pass directly through the bypass switch, completely bypassing the FIP transceivers when the interface is shut down. Most optical bypass switches provide the necessary interface cables for connection to the single-mode or multimode transceivers.

What Is the Cisco 7000 Series?

The FIP provides a 100-Mbps FDDI network interface for Cisco 7000 series routers. Network interfaces reside on modular interface processors, which provide a direct connection between the high-speed Cisco Extended Buses (CxBus) and the external networks.

Figure 6 and Figure 7 show the rear of the Cisco 7000 series routers: the seven-slot model 7000 and the five-slot model 7010. Both use the CxBus. Access to the processor slots and the removable power supplies is from the rear, as shown. Two of the slots are reserved for the Route Processor (RP), which contains the system processor, and the Switch Processor (SP) or Silicon Switch Processor (SSP), each of which performs packet-switching functions. The remaining five (or three) slots, numbered 0 to 4 from left to right (or 0 to 2 from bottom to top), support any combination of network interface types: serial, Ethernet, Fast Ethernet, Token Ring, FDDI, multichannel, channel attachment, or High-Speed Serial Interface (HSSI).

Figure 6 Cisco 7000, Interface Processor End

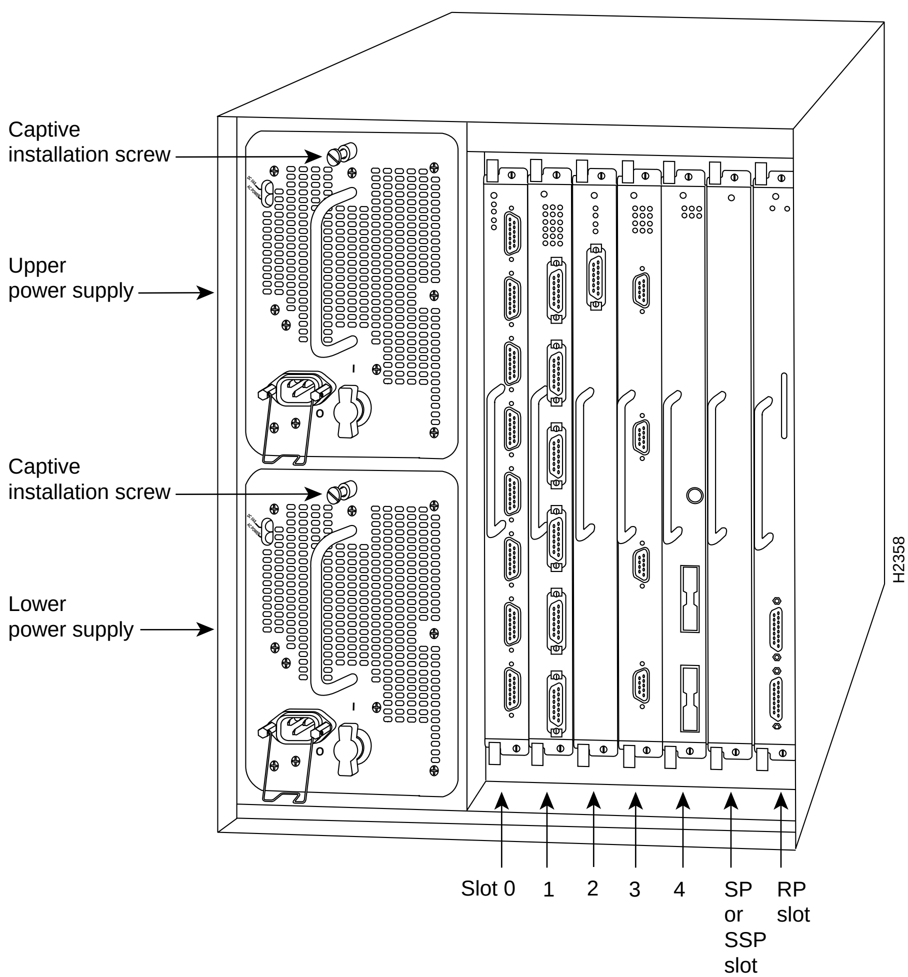
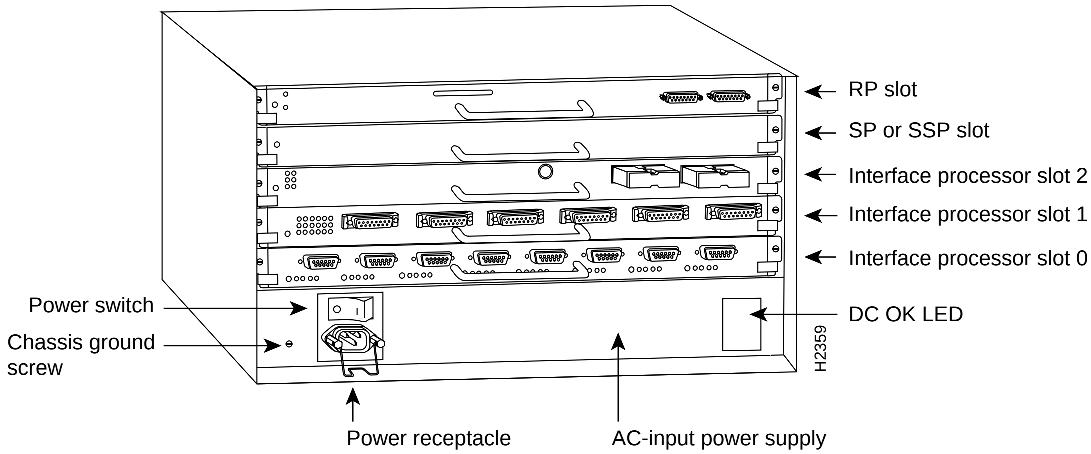


Figure 7 Cisco 7010, Interface Processor End



What Is the Cisco 7500 Series?

The Cisco 7500 series consists of three router models: the Cisco 7505, the Cisco 7507, and the Cisco 7513. All three models provide high reliability, availability, serviceability, and performance. The three systems support multiprotocol, multimedia routing, and bridging with a wide variety of protocols and any combination of Ethernet, Fast Ethernet, Token Ring, FDDI, serial, multichannel, channel attachment, and HSSI media. Network interfaces reside on modular interface processors, which provide a direct connection between the high-speed, 1.067-gigabits-per-second (Gbps) Cisco Extended Bus (CyBus) and the external networks.

Note The Cisco 7507 and Cisco 7513 have dual CyBuses, for an aggregate bandwidth of 2.134 Gpbs.

Figure 8 shows the rear of the five-slot Cisco 7505 router. In the Cisco 7505, one slot (4) is reserved for the Route Switch Processor (RSP1), which contains the system processor and performs packet switching functions. Slots 0 through 3 are for interface processors.

Figure 8 Cisco 7505, Interface Processor End

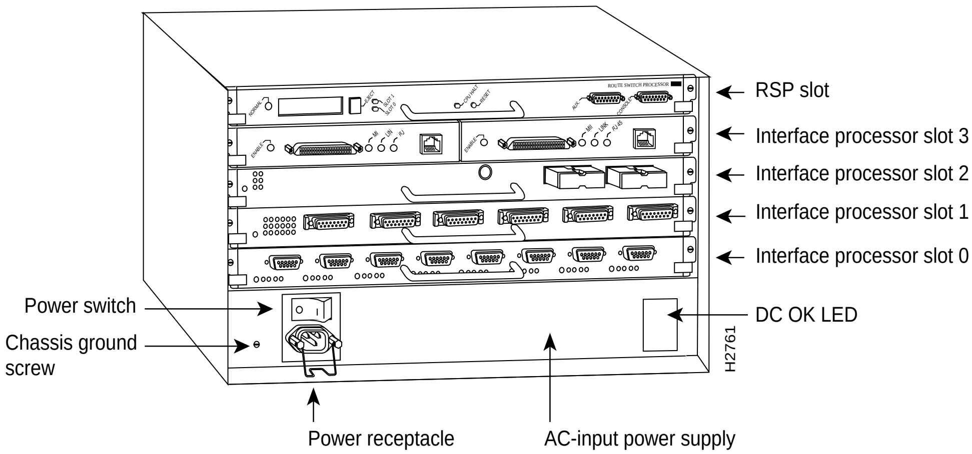


Figure 9 shows the rear of the seven-slot Cisco 7507 router. In the Cisco 7507, up to two slots (2 and 3) are reserved for the Route Switch Processor (RSP2), which contains the system processor and performs packet switching functions. Slots 0 and 1, and 4 through 6 are for interface processors.

Figure 9 Cisco 7507, Interface Processor End

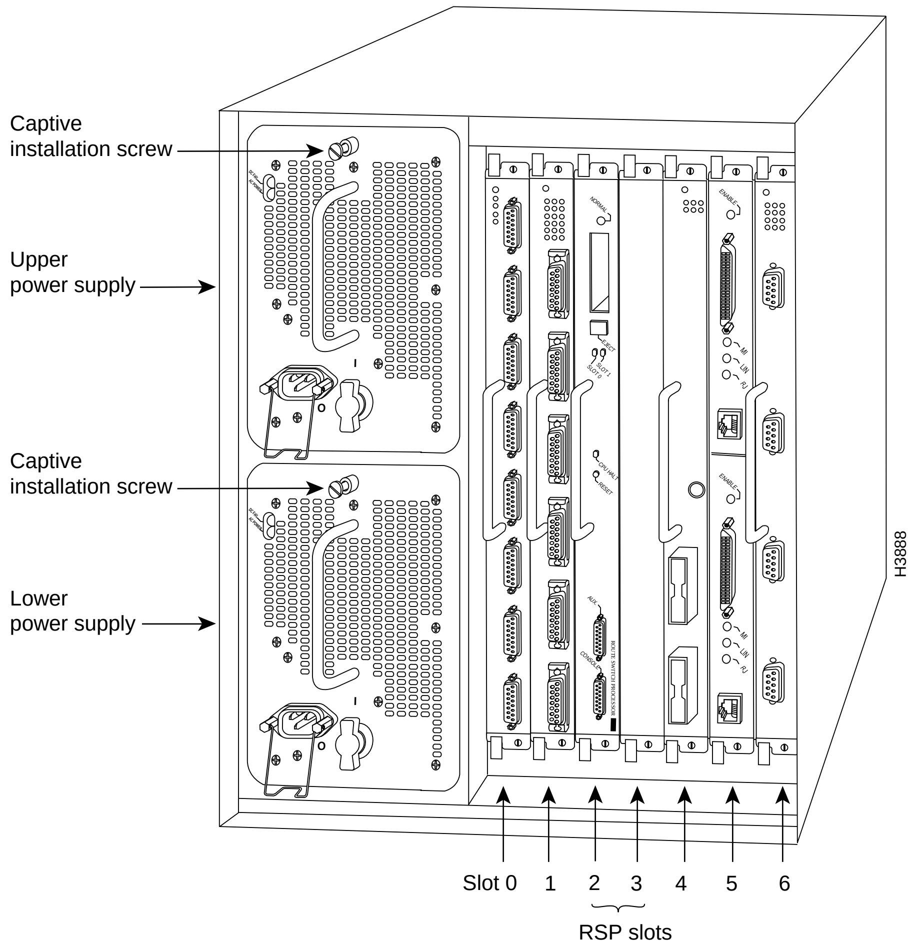
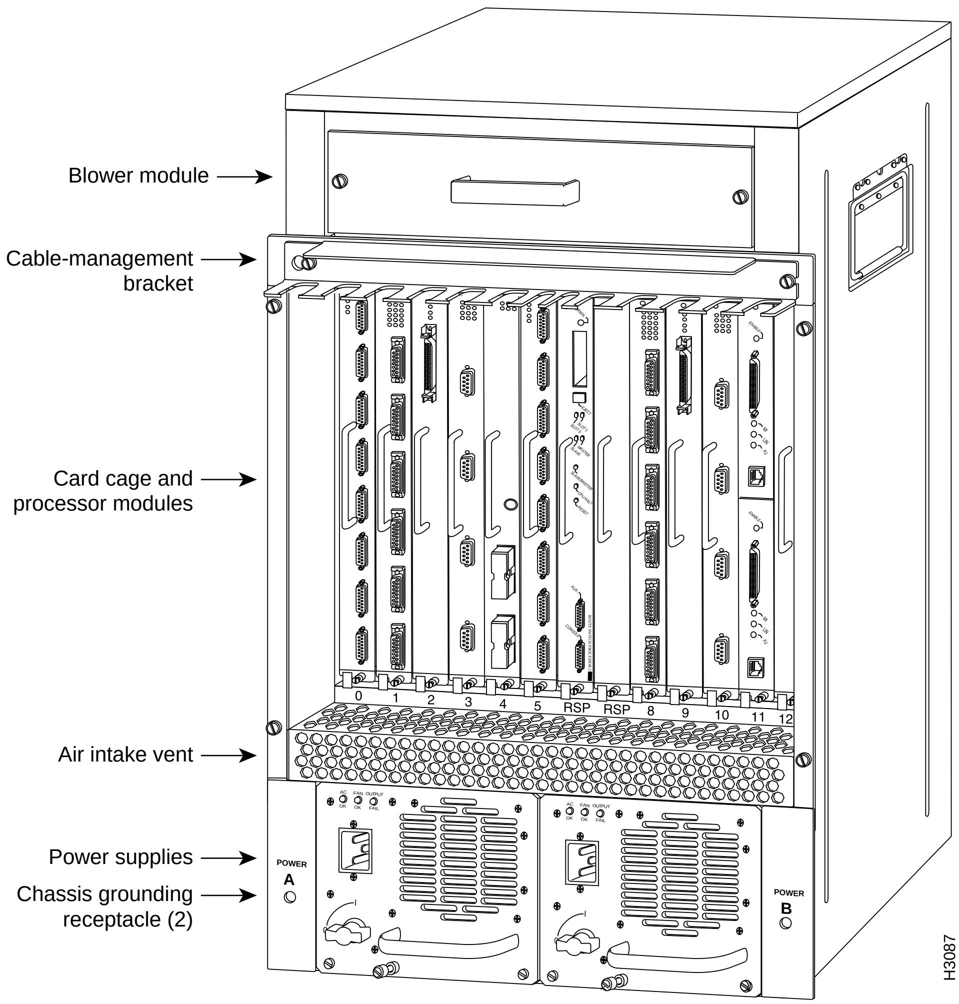


Figure 10 shows the rear of the Cisco 7513, with two AC-input power supplies installed. Two slots (6 and 7) are reserved for the second generation Route Switch Processor (RSP2), which contains the system processor and performs packet switching functions. Slots 0 through 5, and 8 through 12 are for interface processors.

Figure 10   Cisco 7513, Interface Processor End



Installation Prerequisites

Before you begin the installation procedures, review the safety and ESD-prevention guidelines in this section to avoid injuring yourself or damaging the equipment. This section also provides a list of parts and tools you will need to perform the installation.

Distance Limitations for FDDI Connections

The distance limitations for single-mode and multimode FDDI stations are shown in Table 1. If the distance between two connected stations is greater than the maximum distance shown, significant signal loss can result. The single-mode transmitter and the multimode transceiver each provide 11 dB of optical power.

Table 1 FDDI Maximum Transmission Distances

Transceiver Type	Maximum Distance Between Stations
Single-mode	Up to 6.2 miles (up to 10 km)
Multimode	Up to 1.2 miles (up to 2 km)

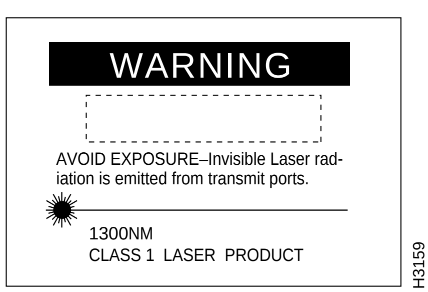
Safety

This section provides special warnings for FDDI transmitter components and safety guidelines you should follow when working with any equipment that connects to electrical power or telephone wiring.

Single-Mode Transmitter

The single-mode transmitter uses a small laser to transmit the light signal to the ring. Keep the transmit port covered whenever a cable is not connected to it. Although multimode transceivers typically use LEDs for transmission, it is good practice to keep open ports covered and avoid staring into open ports or apertures.

Warning Invisible laser radiation may be emitted from the aperture ports of the single-mode FDDI card when no cable is connected. *Avoid exposure and do not stare into open apertures.* Following is an example of the warning label that appears on the product:



Electrical Equipment

Follow these basic guidelines when working with any electrical equipment:

- Before beginning any procedures requiring access to the chassis interior, locate the emergency power-off switch for the room in which you are working.
- Disconnect all power and external cables before moving a chassis.
- Do not work alone when potentially hazardous conditions exist.
- Never assume that power has been disconnected from a circuit; always check.
- Do not perform any action that creates a potential hazard to people or makes the equipment unsafe.
- Carefully examine your work area for possible hazards such as moist floors, ungrounded power extension cables, and missing safety grounds.

Telephone Wiring

Use the following guidelines when working with any equipment that is connected to telephone wiring or to other network cabling:

- Never install telephone wiring during a lightning storm.
- Never install telephone jacks in wet locations unless the jack is specifically designed for wet locations.
- Never touch uninsulated telephone wires or terminals unless the telephone line has been disconnected at the network interface.
- Use caution when installing or modifying telephone lines.

Preventing Electrostatic Discharge Damage

Electrostatic discharge (ESD) damage, which can occur when electronic cards or components are improperly handled, results in complete or intermittent failures. The FIP comprises a printed circuit board that is fixed in a metal carrier. Electromagnetic interference (EMI) shielding, connectors, and a handle are integral components of the carrier. Although the metal carrier helps to protect the board from ESD, use a preventive antistatic strap whenever handling the FIP. Handle the carriers by the handles and the carrier edges only; never touch the boards or connector pins.

Following are guidelines for preventing ESD damage:

- Always use an ESD-preventive wrist or ankle strap and ensure that it makes good skin contact.
- Connect the equipment end of the strap to a captive installation screw on an installed power supply.
- When installing a FIP, use the ejector levers to properly seat the bus connectors in the backplane, then tighten both (top and bottom) captive installation screws. (See Figure 11.) These screws prevent accidental removal, provide proper grounding for the system, and they help to ensure that the bus connectors are seated in the backplane.
- When removing a FIP, use the ejectors to release the bus connectors from the backplane. Use the handle to pull the FIP out slowly while keeping your other hand underneath the carrier to guide it straight out of the slot.
- Handle carriers by the handles and carrier edges only; avoid touching the board or connectors.
- Place a removed FIP board-side-up on an antistatic surface or in a static shielding bag. If the component will be returned to the factory, immediately place it in a static shielding bag.

- Avoid contact between the FIP and clothing. The wrist strap only protects the board from ESD voltages on the body; ESD voltages on clothing can still cause damage.
- Never attempt to remove the FIP printed circuit board from the metal interface processor carrier.

Caution For safety, periodically check the resistance value of the antistatic strap. The measurement should be between 1 and 10 megohms.

Online Insertion and Removal—An Overview

Online insertion and removal (OIR) allows you to remove and replace interface processors while the system is operating; you do not need to notify the software or shut down the system power. This section describes the mechanical functions of the system components and stresses the importance of following the correct procedures to avoid unnecessary restarts or card failures. This section is for background information only. Subsequent sections provide specific procedures for removing and installing an FIP. All CxBus and CyBus interface processors support OIR.

Each processor module contains a bus connector with which it connects to the system backplane. The bus connector is a set of tiered pins, in three lengths. The pins send specific signals to the system as they make contact with the backplane. The system assesses the signals it receives and the order in which it receives them to determine what event is occurring and what task it needs to perform, such as reinitializing new interfaces or shutting down removed ones. For example, when you insert an interface processor, the longest pins make contact with the backplane first, and the shortest pins make contact last. The system recognizes the signals and the sequence in which it receives them. The system expects to receive signals from the individual pins in this logical sequence, and the ejector levers help to ensure that the pins mate in this sequence. When you remove or insert an interface processor, the backplane pins send signals to notify the system, which then performs as follows:

1. Rapidly scans the backplane for configuration changes and does not reset any interfaces.
2. Initializes all newly inserted interface processors, noting any removed interfaces and placing them in the administratively shutdown state.
3. Brings all previously configured interfaces on the interface processor back to the state they were in when they were removed. Any newly inserted interfaces are put in the administratively shut down state, as if they were present (but unconfigured) at boot time. If a similar interface processor type has been reinserted into a slot, then its ports are configured and brought online up to the port count of the original interface processor.

OIR functionality enables you to add, remove, or replace interface processors with the system online, which provides a method that is seamless to end users on the network, maintains all routing information, and ensures session preservation.

When you insert a new interface processor, the system runs a diagnostic test on the new interfaces and compares them to the existing configuration. If this initial diagnostic test fails, the system remains off line for another 15 seconds while it performs a second set of diagnostic tests to determine whether or not the interface processor is faulty and if normal system operation is possible. If the second diagnostic test passes, which indicates that the system is operating normally and the new interface processor is faulty, the system resumes normal operation but leaves the new interfaces disabled.

If the second diagnostic test fails, the system crashes, which usually indicates that the new interface processor has created a problem on the bus and should be removed. The system brings online only interfaces that match the current configuration and were previously configured as up; all other interfaces require that you configure them with the **configure** command. On interface processors with multiple interfaces, only the interfaces that have already been configured are brought online. The new interface remains in the administratively shutdown state until you configure it and bring it online.

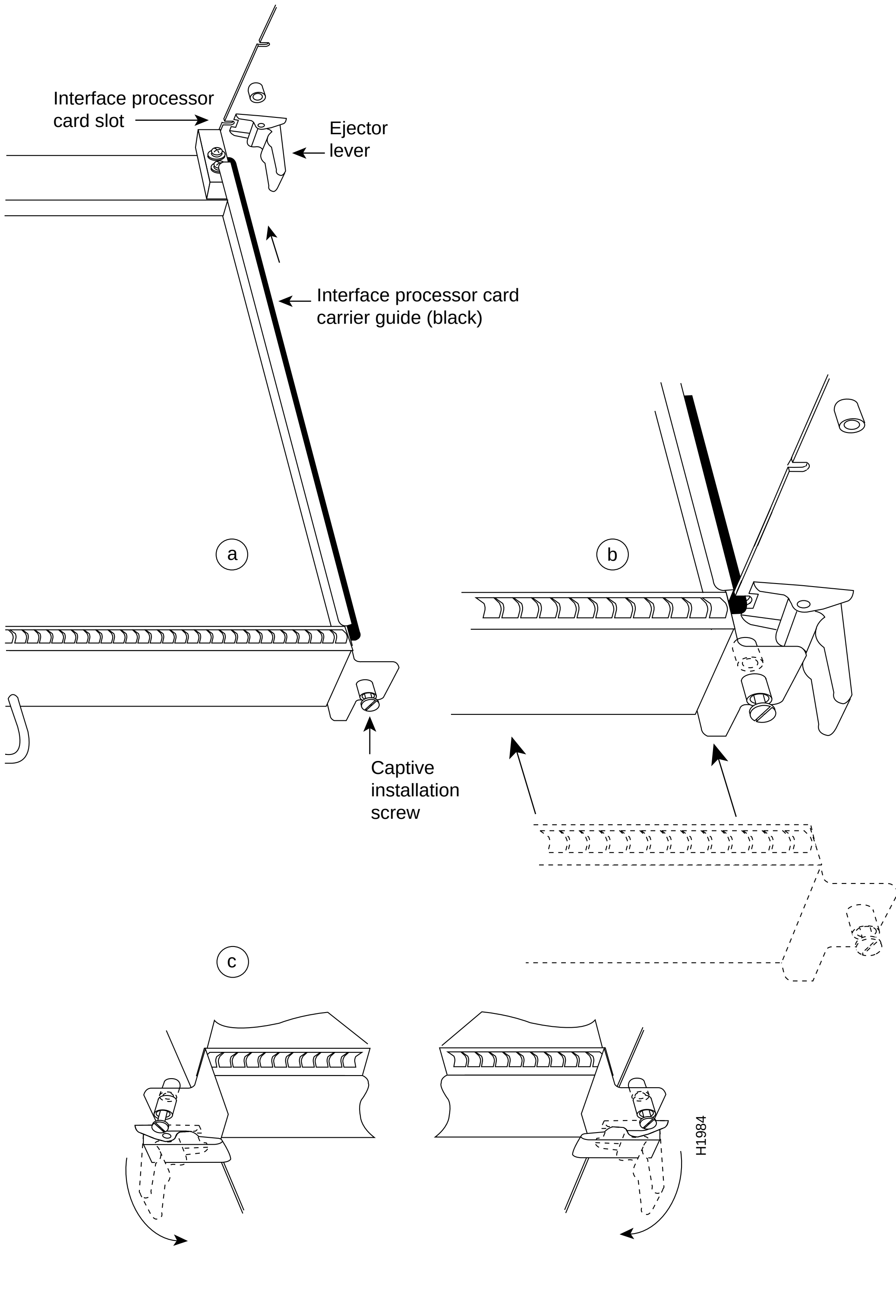
Caution While the FIP supports OIR, the system may indicate a hardware failure if you fail to follow proper procedures.

The function of the ejector levers (see Figure 11) is to align and seat the card connectors in the backplane. Failure to use the ejectors and insert the interface processor properly can disrupt the order in which the pins make contact with the backplane. Follow the FIP installation and removal instructions carefully, and review the following examples of incorrect insertion practices and results:

- Using the handle to force the interface processor all the way into the slot can pop the ejectors out of their springs. If you then try to use the ejectors to seat the interface processor, the first layer of pins (which are already mated to the backplane) can disconnect and then remate with the backplane, which the system interprets as a board failure.
- Using the handle to force or slam the interface processor all the way into the slot can also damage the pins on the board connectors if they are not aligned properly with the backplane.
- When using the handle (rather than the ejectors) to seat the interface processor in the backplane, you may need to pull the interface processor back out and push it in again to align it properly. Even if the connector pins are not damaged, the pins mating with and disconnecting from the backplane will cause the system to interpret a board failure. Using the ejectors ensures that the board connector mates with the backplane in one continuous movement.
- Using the handle to insert or remove an interface processor, or failing to push the ejectors to the full 90-degree position, can leave some (not all) of the connector pins mated to the backplane, a state which will hang the system. Using the ejectors and making sure that they are pushed fully into position ensures that all three layers of pins are mated with (or free from) the backplane.

It is also important to use the ejector levers when removing an interface processor to ensure that the board connector pins disconnect from the backplane in the logical sequence expected by the system. Any processor module that is only partially connected to the backplane can hang the bus. Detailed steps for correctly performing OIR are included with the following procedures for installing and removing a FIP.

Figure 11 Bottom Ejector Lever and Captive Installation Screw



List of Parts and Tools

You need the following tools and parts to install a FIP. If you need additional equipment, contact a customer service representative for ordering information.

- Number 1 Phillips screwdriver for the captive installation screws on the FIP
- External FDDI network interface cables: single-mode or multimode fiber-optic
- Optional: optical bypass switch that can connect to the multimode/multimode FIP (CX-FIP-MM) or the single-mode/single-mode FIP (CX-FIP-SS)
- ESD-prevention equipment or the disposable grounding wrist strap included with all upgrade kits

Installation

The following sections describe the procedures for removing or installing a FIP in the router. The OIR function allows you to install and remove a FIP without shutting down the system power; however, you must follow the insertion instructions carefully. For example, failure to use the ejector levers or insert the FIP properly can cause system error messages indicating a board failure. For a complete description of OIR, refer to the section "Online Insertion and Removal—An Overview" on page 14.

Each unused interface processor slot contains an interface processor filler (which is an interface processor carrier without an interface board) to keep dust out of the chassis and to maintain proper air flow through the interface processor compartment. If you are installing a new FIP that is not a replacement, you must first remove the interface processor filler from an unused slot; proceed to the section "Removing an Interface Processor Filler." If you are replacing a FIP or upgrading the microcode EPROM on a FIP, proceed to the section "Removing a FIP."

Caution To avoid erroneous failure messages, remove or insert only one interface processor at a time. Also, after inserting or removing an interface processor, allow at least 15 seconds before removing or inserting another interface processor so that the system can reinitialize and note the current configuration of all interfaces.

Removing an Interface Processor Filler

Select an unused interface processor slot for the new FIP and remove the interface processor filler as follows:

Step 1 Choose an available slot for the FIP and ensure that there is enough clearance to accommodate any interface equipment that you will connect directly to the ports (for example, transceivers that connect directly to the ports overlap equipment on adjacent interface processors).

Step 2 Use a screwdriver to loosen the captive installation screws on the interface processor filler. (See Figure 11.)

Step 3 Place your thumbs on both ejectors and simultaneously pull them both outward to release the FIP from the backplane connector (in the opposite direction from that shown in Figure 11c).

Step 4 Grasp the handle with one hand and pull the filler straight out of the slot, keeping your other hand under the carrier to guide it. (See Figure 12.) Keep the carrier parallel to the backplane.

Step 5 Store the interface processor filler for future use.

To help prevent dust and contaminants from entering the chassis, do not leave the interface processor slot open. Immediately proceed to the section "Connecting FDDI Interface Cables" on page 21.

Removing a FIP

If you are replacing a failed FIP, remove the existing board first, then replace the new FIP in the same slot. Figure 12 shows proper handling of an interface processor during installation.

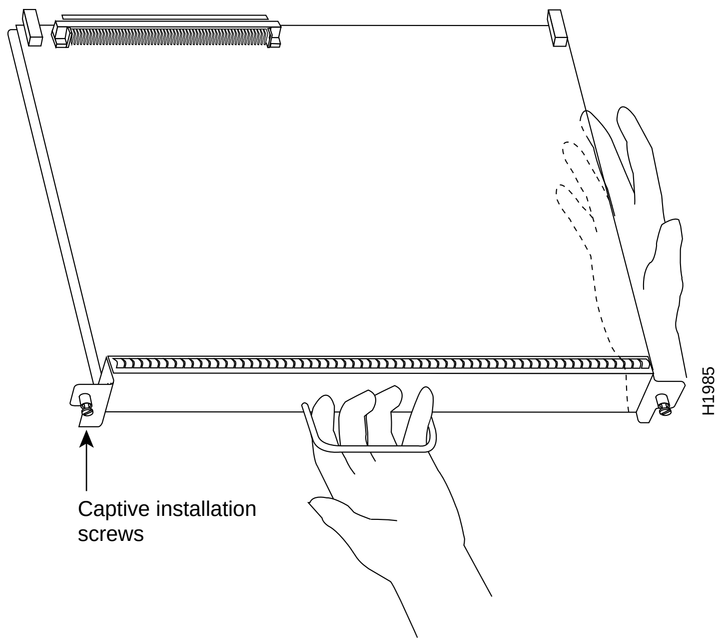
Note Figure 11 shows the functions of the ejector levers in the correct orientation for the horizontal processor slots in a Cisco 7010 and Cisco 7505 chassis. In a Cisco 7000, Cisco 7507, and Cisco 7513 chassis, the function of the ejectors is the same, but the orientation is rotated 90 degrees clockwise for the vertical processor slots.

To remove a FIP, follow these steps:

Step 1 Disconnect the all cables from the FIP ports (if you will are moving the FIP to another port, this step is not necessary).

Step 2 Use a screwdriver to loosen the captive installation screws at both ends of the FIP. (See Figure 12.)

Figure 12 Handling an Interface Processor During Installation and Removal



Caution Always use the ejector levers to remove or install the FIP. Failure to do so can cause erroneous system error messages indicating a board failure.

Step 3 Place your thumbs on the ejector levers and simultaneously pull them outward (in the opposite direction from that show in Figure 11c) to release the FIP from the backplane connector.

Step 4 Use the handle to carefully pull the FIP straight out of the slot, keeping your other hand under the carrier to guide it. (See Figure 12.) Keep the FIP parallel to the backplane.

Step 5 Place the removed FIP on an antistatic mat or foam pad, or place it in an antistatic bag if you will return it to the factory.

Step 6 If the interface processor slot is to remain empty, install an interface processor filler to keep dust out of the chassis and to maintain proper air flow through the interface processor compartment.

Caution To help prevent dust and contaminants from entering the chassis, do not leave the interface processor slot open.

Immediately proceed to the section "Installing a FIP."

Installing a FIP

The FIP slides into the open interface processor slot and directly to the backplane. The interface processors are keyed to guide pins on the backplane, so the FIP can be installed only in an interface processor slot. (The location of interface processor slots depends on your chassis model; refer to Figure 6, Figure 7, Figure 8, Figure 9, or Figure 10). Figure 11 shows the functional details of inserting an interface processor and using the ejectors. Figure 12 shows proper handling of an interface processor during installation.

Caution Remove or insert only one interface processor at a time. Allow at least 15 seconds for the system to complete its discovery and initialization tasks before removing or inserting another interface processor. Disrupting the sequence before the system has completed its verification can cause the system to interpret hardware failures.

Follow these steps to install a FIP:

Step 1 Ensure that the console terminal is connected to the RP (or RSP) *Console* port and that the console is turned ON.

Step 2 Hold the FIP handle with one hand, and place your other hand under the carrier to support the FIP and guide it into the slot. (See Figure 12.) Avoid touching the card or any connector pins.

Caution To prevent ESD damage, wear an ESD-preventive wrist strap and handle interface processors by the handles and carrier edges only.

Step 3 Place the back of the FIP in the slot and align the notch on the carrier with the groove in the slot. (See Figure 11.)

Step 4 Keep the FIP carrier parallel to the backplane, and slide it into the slot until the back of the faceplate makes contact with the ejector levers, then *stop*. (See Figure 11b.)

Caution Always use the ejector levers when installing or removing processor modules. A module that is partially seated in the backplane will cause the system to hang and subsequently crash, and shoving or slamming the interface processor into the slot can damage the backplane and connector pins.

Step 5 Using your thumbs, simultaneously push both ejectors inward until the FIP is pushed entirely into its slot. (See Figure 11c.)

Step 6 Tighten the captive screws on the ends of the interface processor faceplate to prevent the interface processor from becoming partially dislodged from the backplane and ensure proper EMI shielding. (These screws must be tightened to meet EMI specifications.)

Proceed to the following section to attach network interface cables.

Connecting FDDI Interface Cables

Following are detailed instructions for connecting the FIP as either a single attachment or dual attachment station to both single-mode and multimode networks. Single-mode uses separate transmit and receive cables. You will need two single-mode cables for a single attachment connection or four cables for a dual attachment connection. Multimode uses one integrated transmit/receive cable for each physical interface (one for PHY A and one for PHY B). You will need one multimode cable for a single attachment connection, and two cables for a dual attachment connection. Figure 18, which shows the connections for a dual attachment connection that uses both single-mode and multimode fiber, illustrates the types of connections used for both fiber modes. For cable and connector descriptions, refer to the section "FDDI Transceivers and Connectors" on page 6.

Note Each station in a ring refers to its neighbor stations as *upstream* or *downstream* neighbors. The *stream* is based on the signal flow on the primary ring. A station receives the primary signal from its upstream neighbor, and transmits the primary signal to its downstream neighbor. For example, Figure 2 shows the primary signal flow being transmitted from PHY B on Station 2 to PHY A on Station 1, and from PHY B on Station 1 to PHY A on Station 4. Using Station 1 as a reference, Station 2 is the upstream neighbor of Station 1, and Station 4 is the downstream neighbor of Station 1.

This section also provides instructions for connecting an optical bypass switch to a dual attachment multimode network connection. Because the method of connecting optical bypass switches varies between different manufacturer's models, refer to the documentation for your particular bypass switch for correct connection instructions. If you are installing an optical bypass switch, proceed to the section "Installing an Optical Bypass Switch" on page 26.

Warning Invisible laser radiation may be emitted from the aperture ports of the single-mode FDDI products when no fiber cable is connected. *Avoid exposure and do not stare into open apertures*. This product meets the Class 1 Laser Emission Requirement from the CDRH FDDI.

Single Attachment Connections

A FIP that is connected as a single attachment station typically is connected to the ring through a concentrator. The FIP receives and transmits the signal through the same physical interface, usually PHY A. Depending upon whether you are connecting to a single-mode of multimode fiber network, connect the FIP as follows:

- Single-mode—Connect one single-mode interface cable to the PHY A transmit port, and one to the PHY A receive port. (See Figure 13.) Connect the opposite end of each cable to the concentrator transmit and receive ports as specified by the concentrator manufacturer.
- Multimode—Connect the multimode interface cable between one of the M ports on the concentrator and the PHY A port on the FIP. (See Figure 14.) Be sure to observe and match the port labels on the MIC and the FIP ports; connect receive on the cable to PHY A receive. Follow the concentrator manufacturer's instructions for connecting the opposite end of the cable.

If you are connecting other FIPs as dual attachment stations, proceed to the following section. Otherwise, proceed to the section "Checking the Installation" on page 27.

Figure 13 SAS, Single-Mode Fiber Network Connections (CX-FIP-SS)

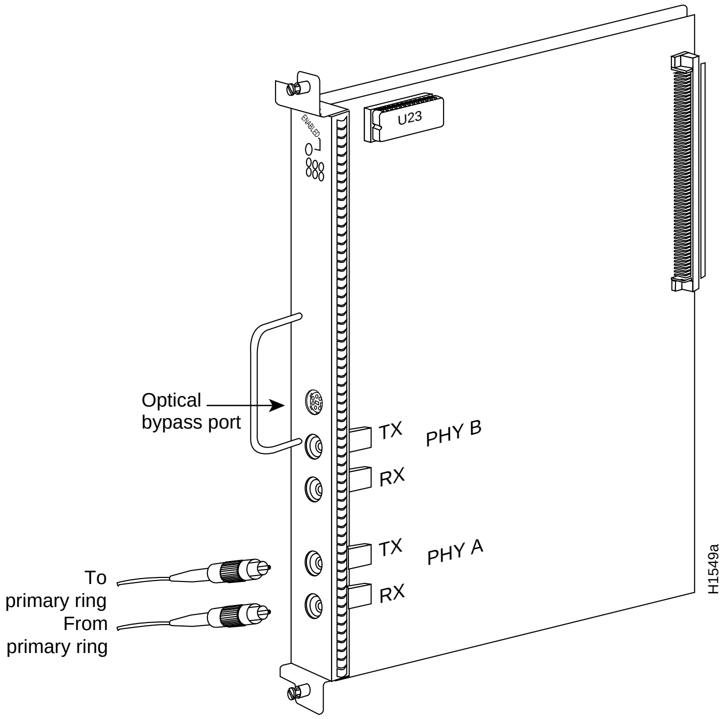
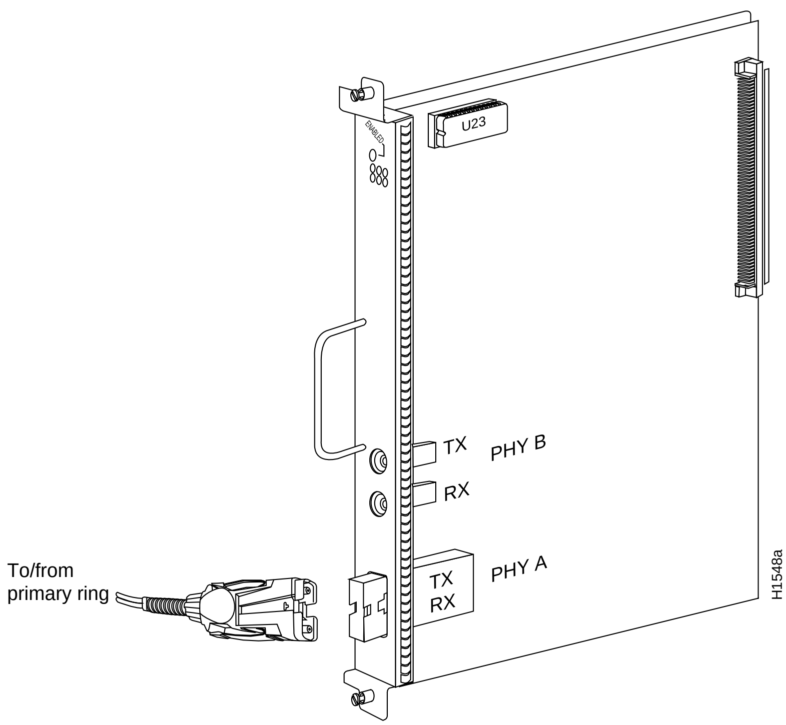


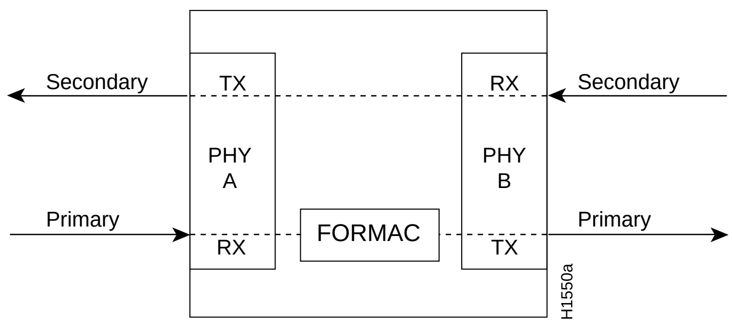
Figure 14 SAS, Multimode Fiber Network Connections (CX-FIP-SM)



Dual Attachment Connections

A FIP that is connected as a dual attachment station connects to both the primary and secondary rings. The signal for each ring is received on one physical interface (PHY A or PHY B) and transmitted from the other. The standard connection scheme (shown in Figure 15) for a dual attachment station dictates that the primary ring signal comes into the FIP on the PHY A receive port and returns to the primary ring from the PHY B transmit port. The secondary ring signal comes into the FIP on the PHY B receive port returns to the primary ring from the PHY A transmit port. Failure to observe this relationship will prevent the FDDI interface from initializing. Figure 18 shows the connections for a dual attachment that uses both multimode and single-mode fiber.

Figure 15 FDDI DAS Ports



Depending upon whether you are connecting to a single-mode or multimode fiber network, connect the FIP as follows:

- Single-mode—Observe the standard connection scheme described previously and refer to Figure 16 while you connect the interface cables as follows:
  - — Connect the cable coming in from the primary ring (*from* PHY B at the primary ring upstream station) to the FIP PHY A receive port.
  - — Connect the cable going out to the primary ring (*to* PHY A at the primary ring downstream station) to the FIP PHY B transmit port.
  - — Connect the cable coming in from the secondary ring to the FIP PHY B receive port.
  - — Connect the cable going out to the secondary ring to the FIP PHY A transmit port.
- Multimode—Each of the integrated transmit/receive multimode interface cables attaches to both the primary and secondary ring; each one receives the signal from one ring and transmits to the other ring. (See Figure 17.) To help avoid confusion, use the receive label on the cable MIC connector as a key and connect the cables to the FIP ports as follows:
  - — Connect the cable coming in from the primary ring to the PHY A receive port. This also connects the signal going out to the secondary ring to the PHY A transmit port.
  - — Connect the cable coming in from the secondary ring to the PHY B receive port. This also connects the signal going out to the primary ring to the PHY B transmit port.

If you are connecting other FIPs to an optical bypass switch, proceed to the next section. Otherwise, proceed to the section "Checking the Installation" on page 27.

Figure 16 DAS, Single-Mode Fiber Network Connections (CX-FIP-SS)

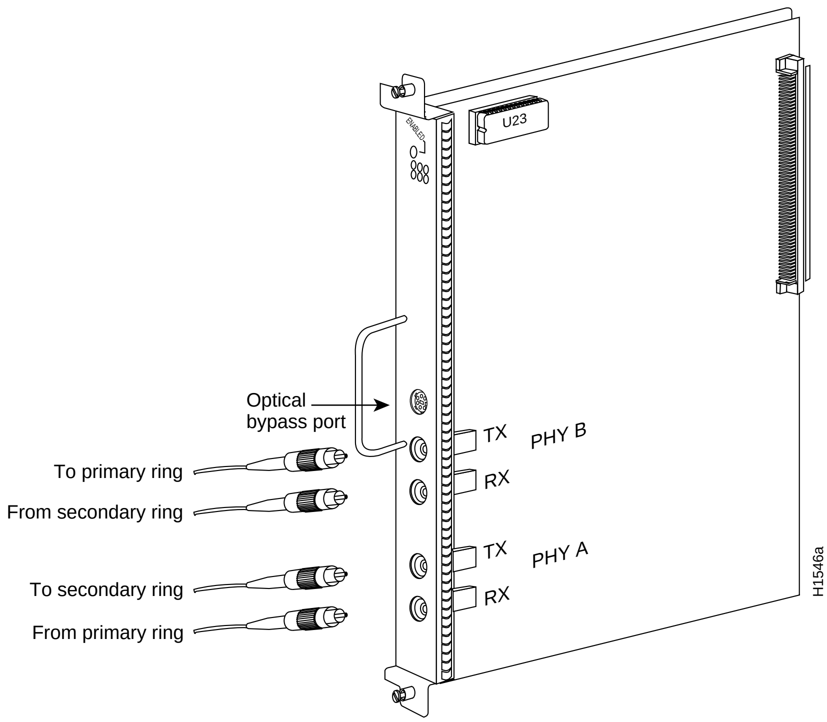
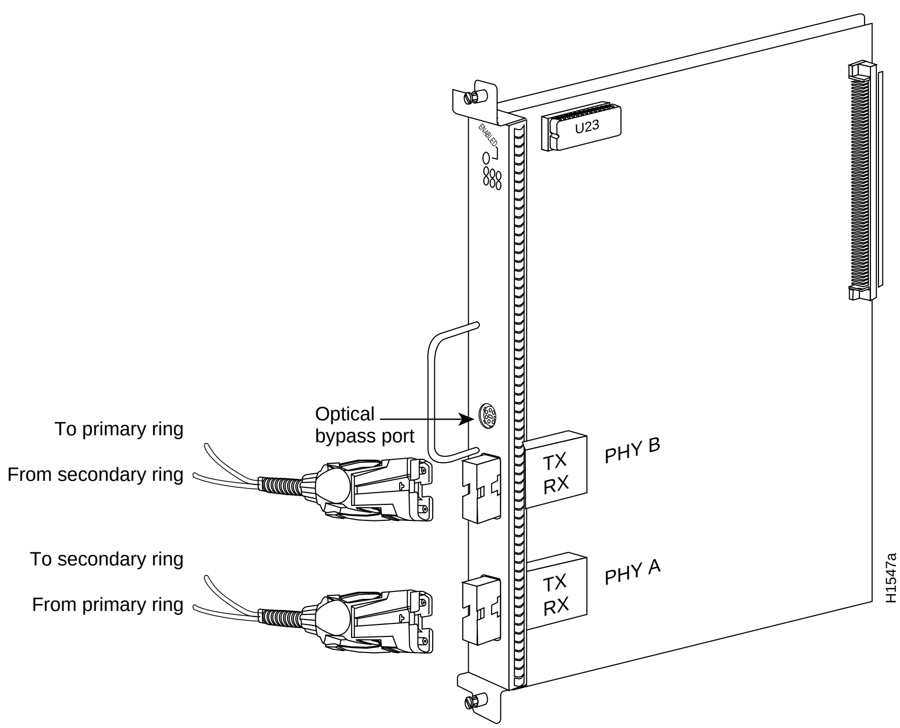


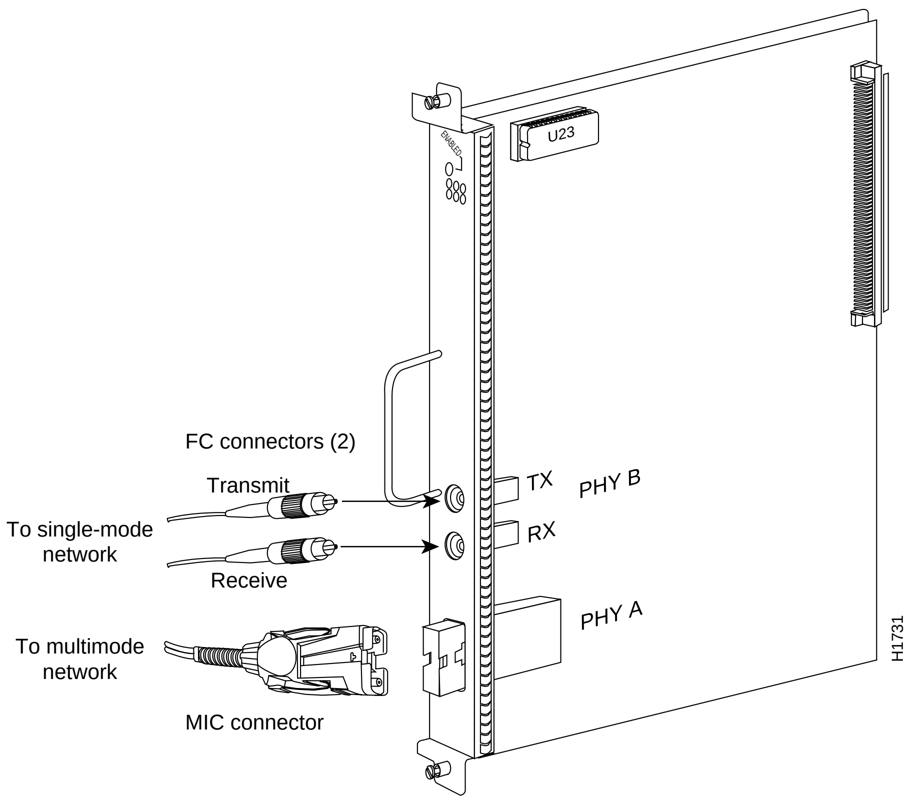
Figure 17 DAS, Multimode Fiber Network Connections (CX-FIP-MM)



- Mixed mode—Follow the cabling guidelines described previously to connect the multimode and single-mode interface cables. Figure 18 shows that the primary ring signal is received on the multimode PHY A receive port and transmitted from the single-mode PHY B transmit port. Your configuration may be opposite, with multimode on PHY B and single-mode on PHY A. Connect the cables to the FIP ports as follows:
    - Connect the cable coming in from the primary ring to the PHY A receive port, and connect the signal going out to the secondary ring to the PHY A transmit port.
    - Connect the cable coming in from the secondary ring to the PHY B receive port. This also connects the signal going out to the primary ring to the PHY B transmit port.

If you are connecting other FIPs to an optical bypass switch, proceed to the next section. Otherwise, proceed to the section “Checking the Installation” on page 27.

Figure 18 DAS Connection, Mixed Mode (CX-FIP-SM)



Note The CX-FIP-MS could also be used for DAS mixed-mode connections, which would be the opposite of those shown for the CX-FIP-SM in Figure 18: PHY-A would connect to a single-mode network and PHY-B would connect to a multimode network.

Installing an Optical Bypass Switch

An optical bypass switch is a device installed between the ring and the station that provides additional fault tolerance to the network. If a FIP that is connected to a bypass switch fails or shuts down, the bypass switch activates automatically and allows the light signal to pass directly through it, bypassing the FIP completely. A port for connecting an optical bypass switch is provided on the multimode/multimode FIP (CX-FIP-MM, shown in Figure 19), and the single-mode/single-mode FIP (CX-FIP-SS, shown in Figure 20).

Figure 19 Optical Bypass Switch Connection (CX-FIP-MM)

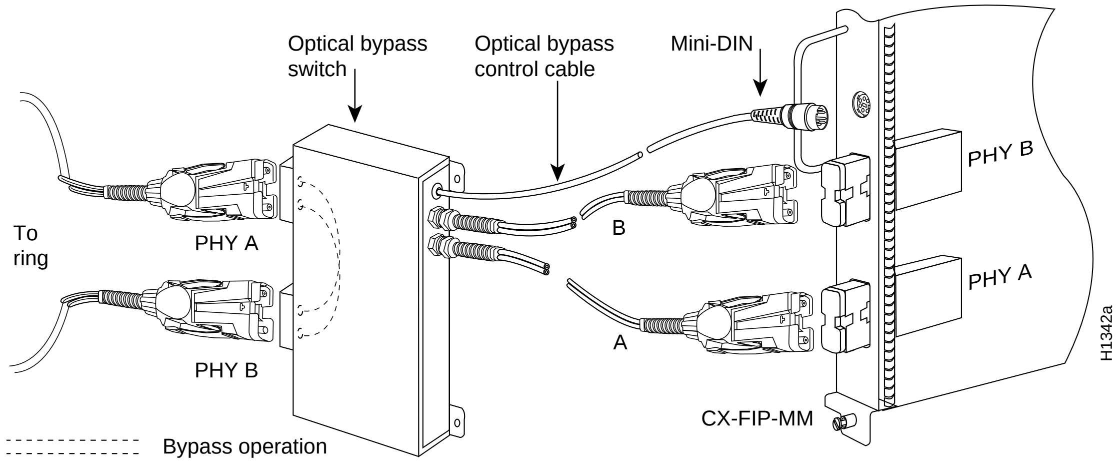
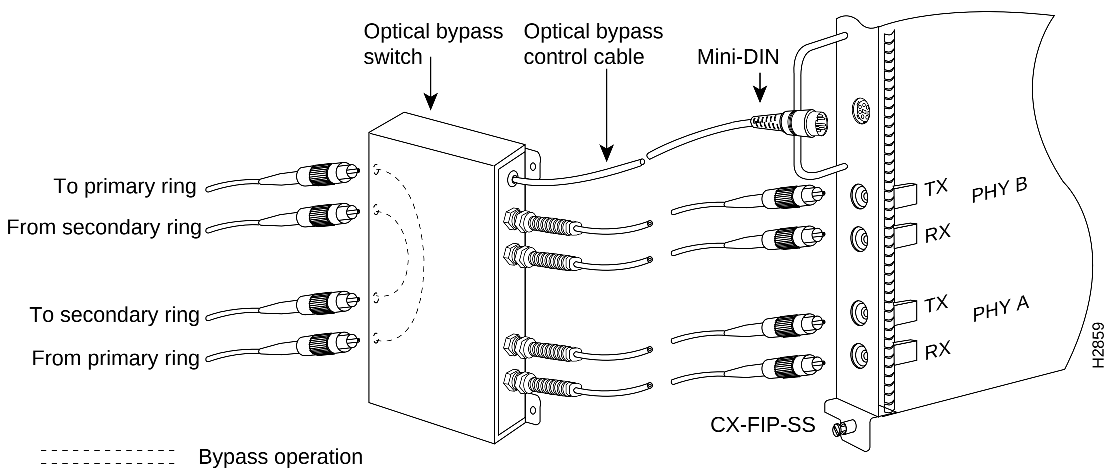


Figure 20 Optical Bypass Switch Connection (CX-FIP-SS)



Note Up to 100 milliamperes of current can be supplied to the optical bypass switch.

Following are general instructions for connecting an optical bypass switch to the FIP; however, your particular bypass switch may require a different connection scheme. Use these steps and the illustrations in Figure 19 and Figure 20, on page page 26, as general guidelines, but for specific connection requirements, refer to the instructions provided by the manufacturer of the switch.

- Connect the bypass switch to the ring. Unless the documentation that accompanies the bypass switch instructs otherwise, observe the same guidelines for connecting the A/B ports on the bypass switch that you would to connect the ring directly to the FIP ports. Use the receive label on the cable connectors as a key and connect the multimode or single-mode cables to the network (ring) side of the bypass switch as follows:
  - — Connect the cable coming in from the primary ring (*from* PHY B at the preceding station) to the PHY A receive port on the network (ring) side of the bypass switch. This also connects the signal going out to the secondary ring to the PHY A transmit port.
  - — Connect the cable coming in from the secondary ring (*from* PHY A at the preceding station) to the PHY B receive port on the network (ring) side of the bypass switch. This also connects the signal going out to the primary ring to the PHY B transmit port.
- Connect the bypass switch to the FIP. Unless the documentation that accompanies the bypass switch instructs otherwise, consider the bypass an extension of the FIP ports and connect A to A and B to B. The network cables are already connected to the bypass switch following the standard B-to-A/A-to-B scheme.
  - — Connect an interface cable between the PHY A port on the station (FIP) side of the bypass switch and the FIP PHY A port.
  - — Connect an interface cable between the PHY B port on the station (FIP) side of the bypass switch and the FIP PHY B port.
- Connect the bypass switch control cable. If the control cable on your optical bypass switch uses a mini-DIN connector, connect the cable directly to the female mini-DIN optical bypass port on the FIP. If the switch uses a standard DIN connector, use the optical bypass adapter cable (CAB-FMDD=) supplied with each FIP. Connect the DIN end of the adapter cable to the DIN on the control cable, and connect the mini-DIN end of adapter cable to the mini-DIN optical bypass port on the FIP.

Proceed to the following section to check the installation.

Checking the Installation

After you install the FIP, verify the installation by observing the LED states and the console display. When the system has reinitialized all interfaces, the enabled LED on the FIP and on all interface processors should go on. The console screen will also display a message as the system discovers each interface during its reinitialization.

When you remove and replace interface processors, the system provides status messages on the console screen. The messages are for information only.

The following sample display shows the events logged by the system as a FIP was removed from slot 1; the system then reinitialized the remaining interface processors and marked as *down* the FDDI interface on the FIP that was removed from slot 1. When a new FIP was reinserted, the system automatically brought up the interface because it was up when the FIP was removed.

```
Router#

%OIR-6-REMCARD: Card removed from slot 1, interfaces disabled
%LINK-5-CHANGED: Interface Fddi1/0, changed state to administratively down

Router#
%OIR-6-INSCARD: Card inserted in slot 1, interfaces administratively shut down
%LINK-5-CHANGED: Interface Fddi1/0, changed state to up
```

When a new FIP is inserted or when a FIP is moved to a new slot, the system recognizes the new FDDI interface, but leaves the interface in a *down* state until you configure it and change the state to *up* with the **configure** command. The following example display shows the events logged by the system as a new FIP is inserted in slot 3:

```
Router#
%OIR-6-INSCARD: Card inserted in slot 3, interfaces administratively shut down
```

Verify that the FIP is installed correctly as follows:

Step 1 While the system reinitializes each interface, observe the console display messages and verify that the system discovers the FIP as follows:

- If you installed a new FIP, the system should recognize the new FDDI interface but leave it configured as *down*.
- If you replaced a FIP, the system should recognize each interface and place it in the same state (*up* or *down*) each was in when you removed the FIP.

Step 2 When the reinitialization is complete, verify that the enabled LED on the FIP goes on and remains on. If it does, proceed to step 5. If it does not, proceed to the next step.

Step 3 If the enabled LED on the FIP fails to go on, suspect that the FIP board connector is not fully seated in the backplane. Loosen the captive installation screws, then firmly push the top ejector down while pushing the bottom ejector up until both are parallel to the FIP faceplate. Tighten the captive installation screws. After the system reinitializes the interfaces, the enabled LED on the FIP should go on. If it does, proceed to step 5. If it does not, proceed to the next step.

Step 4 If the enabled LED still fails to go on, remove the FIP and try installing it in another available interface processor slot.

- If the enabled LED goes on when the FIP is installed in the new slot, suspect a failed backplane connection in the original interface processor slot.
- If the enabled LED still fails to go on, but other LEDs on the FIP go on to indicate activity, proceed to step 5 to resume the installation checkout and suspect that the enabled LED on the FIP has failed.
- If no LEDs on the FIP go on, suspect that the FIP is faulty.
- If the enabled LED still does not go on, do not proceed with the installation. Contact a service representative to report the problem and obtain further instructions. Instructions for obtaining technical assistance are provided at the end of this document.

Step 5 If the FIP is new and not a replacement, proceed to the section “Configuring the FDDI Interface” on page 29 to configure the new FDDI interface. (This does not have to be done immediately, but new interface will not be available until you configure it.)

Step 6 If this installation was a replacement FIP, proceed to the section “Checking the Configuration” on page 31, to verify the status of the interface.

If you experience problems that you are unable to solve, contact a service representative for assistance.

Configuring the FDDI Interface

If you installed a new FIP or if you want to change the configuration of an existing interface, you must enter the configuration mode. If you replaced an FIP that was previously configured, the system will recognize the new FIP interfaces and bring each of them up in their existing configuration.

After you verify that the new FIP is installed correctly (the enabled LED goes on), use the privileged-level **configure** command to configure the new interfaces. Be prepared with the information you will need, such as the following:

- Protocols you plan to route on the new interface
- Internet Protocol (IP) addresses if you are configuring the interface for IP routing
- Whether or not the new interfaces will use bridging

Refer to the *Router Products Configuration Guide* publication for a summary of the configuration options available and instructions for configuring FDDI interfaces.

Note The **configure** command requires privileged-level access to the EXEC command interpreter, which usually requires a password. Contact your system administrator to obtain EXEC-level access.

Using the EXEC Command Interpreter

Before you use the **configure** command, you must enter the privileged level of the EXEC command interpreter with the **enable** command. The system will prompt you for a password if one has been set.

The system prompt for the privileged level ends with a pound sign (#) instead of an angle bracket (>). At the console terminal, enter the privileged level as follows:

Step 1 At the user-level EXEC prompt, enter the **enable** command. The EXEC prompts you for a privileged-level password, as follows:

```
Router> enable

Password:
```

Step 2 Enter the password (the password is case-sensitive). For security purposes, the password is not displayed.

Step 3 When you enter the correct password, the system displays the privileged-mode system prompt (#) as follows:

```
Router#
```

Proceed to the following section to configure the new interfaces.

Using the Configure Command

Following are instructions for a basic configuration: enabling an interface and specifying IP routing on an FDDI interface. You might also need to enter other configuration subcommands, depending upon the requirements for your system configuration and the protocols you plan to route on the interface. For complete descriptions of configuration subcommands and the configuration options available for FDDI interfaces, refer to the *Router Products Configuration Guide*.

Cisco 7000 series and 7500 series routers identify an interface address by its slot number and port number in the format *slot/port*. Each FIP contains one interface, which is always port (interface) 0. For example, the slot/port address of the FDDI interface on a FIP installed in interface processor slot 1 is *1/0*. The address of an FDDI port on a FIP in slot 2 would be *2/0*. The following section describes a basic configuration.

Basic Configuration

Following are instructions for a basic configuration: enabling FDDI interfaces and specifying IP routing. You might also need to enter other configuration subcommands, depending upon the requirements for your system configuration (configuration subcommands are described in the *Router Products Command Reference* publication). Press the Return key after each configuration step unless otherwise noted.

Step 1 At the privileged-level prompt, enter the configuration mode and specify that the console terminal will be the source of the configuration subcommands as follows:

```
Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z
Router(config)#
```

Step 2 At the prompt, specify the first interface to configure by entering the subcommand **interface**, followed by the *type* (**fddi**) *and slot/port* (interface processor slot number/0). The example that follows is for the FDDI port on a FIP in interface processor slot 2:

```
Router(config)# interface fddi 2/0
```

Step 3 If IP routing is enabled on the system, you can assign an IP address and subnet mask to the interface with the **ip address** configuration subcommand as in the following example:

```
Router(config-int)# ip address 145.1.1.1 255.255.255.0
```

Step 4 Add any additional configuration subcommands required to enable routing protocols and adjust the interface characteristics.

Step 5 Change the default shutdown state to up and enable the interface as follows:

```
Router(config-int)# no shutdown
```

Step 6 When you have included all of the configuration subcommands to complete the configuration, press **Ctrl-Z** (hold down the Control key while you press z) to exit the configuration mode.

Step 7 Write the new configuration to memory as follows:

```
Router# copy running-config startup-config
```

The system will display an OK message when the configuration has been stored.

Step 8 Exit privileged level and return to user level by entering **disable** at the prompt as follows:

```
Router# disable
```

Proceed to the following section to check the interface configuration with **show** commands.

Checking the Configuration

After configuring the new interface, use the **show** commands and status LEDs to check the status of the new interface or all interfaces.

Command Descriptions and Examples

Following are descriptions and examples of the **show** commands. Descriptions are limited to fields that are relevant for verifying the configuration.

- **show version** displays the configuration of the system hardware (the number of each interface processor type installed), the software version, the names and sources of configuration files, and the boot images.

```
Router> show version

GS Software (GS7), Version 10.3(5)
Copyright (c) 1986-1995 by cisco Systems, Inc.
Compiled Wed 10-May-95 14:44

System Bootstrap, Version 4.6(1)

Current date and time is Fri 2-26-1993 2:18:52
Boot date and time is Fri 1-29-1993 11:42:38
Router uptime is 3 weeks, 6 days, 14 hours, 36 minutes
System restarted by power-on
Running default software
Network configuration file is "Router", booted via tftp from 1.1.1.333

RP1 (68040) processor with 16384K bytes of memory.
X.25 software, Version 2.0.
Bridging software.
1 Switch Processor.
1 EIP controller (6 Ethernet).
1 TRIP controller (4 Token Ring).
6 Ethernet/IEEE 802.3 interface.
(display text omitted)
```

- **show protocols** displays the global (system-wide) and interface-specific status of any configured Level 3 protocol.

```
Router> show protocols

Global values:
  Internet Protocol routing is enabled
Serial1/0 is up, line protocol is up

(display text omitted)
```

- **show configuration** displays the contents of the system configuration file stored in NVRAM. This file should reflect all new configuration changes you made and wrote to memory with the **write terminal** command.

```
Router# show config

Using 1652 out of 130048 bytes
version 10.3(5)
!
hostname Router
!
enable-password guessagain
!
microcode TRIP flash fip10-0
microcode reload
(display text omitted)
!
interface Fddi3/0
ip address 1.1.1.14 255.255.255.0
ip route-cache cbus
no keepalive
novell network 1033
!
(display text omitted)
```

- **show controllers cxbus** displays the internal status of each interface processor, including the interface processor slot location, the card hardware version, and the currently running microcode version. It also lists each interface (port) on each interface processor including the logical interface number, interface type, physical (slot/port) address, and hardware (station address) of each interface. This example shows an FIP installed in interface processor slot 3:`

```
Router> show cont cxbus

(display text omitted)

FIP 3, hardware version 1.3, microcode version 141.12
  Interface 24 - Fddi3/0, station addr 0000.0c02.adf1 (bia 0000.0c02.adf1)
    13 buffer RX queue threshold, 33 buffer TX queue limit, buffer size 4484
    ift 0006, rql 9, tq 0000 0000, tql 32
    (display text omitted)
```

- **show interfaces fddi** *slot/port* displays statistics for the FDDI interface you specify by its slot/port address. If you use this command without the *type* and *slot/port* arguments, the system will display statistics for all interfaces in the system. The following example show a FIP installed in slot 3:

```
Router> show int fddi3/0

Fddi3/0 is up, line protocol is up
  Hardware is cxBus Fddi, address is 0000.0c02.adf1 (bia 0000.0c02.adf1)
  Internet address is 1.1.1.14, 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
  CFM is thru A, token rotation 5000 usec, ring operational 15:25:31
  Upstream neighbor 0000.0c01.261a, downstream neighbor 0000.0c01.4117
  (display text omitted)
```

Using Show Commands to Verify the FIP Status

The following procedure describes how to use the **show** commands to verify that the new interface is configured correctly:

Step 1 Display the system hardware configuration with the **show version** command. Ensure that the list includes any new or replaced FDDI interfaces.

Step 2 Display all the current interface processors and their interfaces with the **show controllers cxbus** command. Verify that the new FIP appears in the correct slot.

Step 3 Specify a new FDDI interface with the **show interfaces fddi** *slot/port* command and verify that the first line of the display specifies the interface with the correct slot number. Also verify that the interface and line protocol are in the correct state: up or down.

Step 4 Display the protocols configured for the entire system and specific interfaces with the command **show protocols**. If necessary, return to the configuration mode to add or remove protocol routing on the system or specific interfaces.

Step 5 Display the entire system configuration file with the **show configuration** command. Verify that the configuration is accurate for the system and each interface.

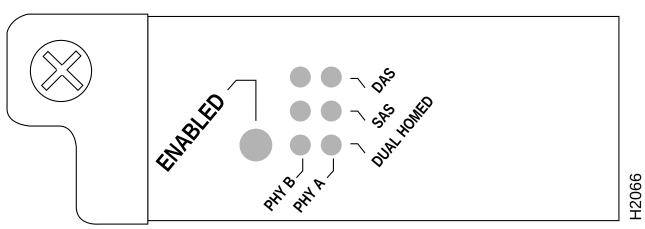
If the new interface is down and you configured it as up, or if the displays indicate that the hardware is not functioning properly, ensure that the FDDI network interface cables are properly connected. If you still have problems bringing the interface up, contact a service representative for assistance.

Proceed to the following section to check the status of the new FDDI interface by observing the status LEDs on the FIP.

Checking the LEDs

The FIP contains the bank of LEDs shown in Figure 21.

Figure 21 FIP LEDs



The enabled LED goes on to indicate that the FIP is operational and that it is enabled for operation. It does *not* mean that the interface ports are functional or enabled. The left vertical row of three LEDs indicates the status of PHY B, the right vertical of three LEDs indicates the status of PHY A (the PHY B interface is located next the PHY A interface on the face of the FIP). The state of each B/A pair of LEDs indicates the status of one type of three possible station connections: DAS, SAS, or dual homed.

The following conditions must be met before the FIP is enabled:

- The FIP is correctly connected to the backplane and receiving power.
- The FIP contains a valid microcode version that has successfully been downloaded.
- The bus recognizes the FIP.

If any one of these conditions is not met, or if the initialization fails, the enabled LED does not go on.

The states of the FIP LED combinations, and the meanings of each are described and illustrated in Table 2.

Table 2 FIP LED States, Refer to Figure 21

LED Pattern[1]	State	Indication
B A	**DAS**	
– – X X X X	Both lights off	Not connected
O O X X X X	Both lights on	Through A
O – X X X X	B on and A off	Wrap B
– O X X X X	B off and A on	Wrap A
B A	**SAS**	
X X – – X X	Both lights off	Not connected
X X O – X X	B on and A off	Single attachment B (PHY A shut down)
X X – O X X	B off and A on	Single attachment A (PHY B shut down)
B A	**Dual Homed**	
X X X X – –	Dual homed B and A off	Not connected
X X X O O O	Single attachment A on Dual homed B and A on	Dual homed with A active; not a normal condition; indicates potential problem on B
X X O X O O	Single attachment B on Dual homed B and A on	Dual homed with B active, which is a normal condition
X X O X O X	Single attachment B on Dual homed B on	Single attachment B Dual homed A failed
X X X O X O	Single attachment A on Dual homed A on	Single attachment A Dual homed B failed

1. For the LED patterns "–" means off, "O" means on, and "X" means does not apply. Refer to Figure 21.

Upgrading Microcode

The Cisco 7000 series and Cisco 7500 series support downloadable microcode, which enables you to upgrade microcode versions without having to physically replace the EPROMs on the boards. You can download new microcode versions and store multiple versions in Flash memory, and you can boot from them just as you can with the system software images. System software upgrades may also contain upgraded microcode images, which will load automatically when the new software image is loaded.

This section describes how to use and configure downloadable microcode and, if necessary, how to replace the microcode EPROM on the FIP.

Downloading Microcode to Flash Memory

You can download microcode to Flash memory by copying the TFTP image of a microcode version to Flash memory. When the microcode image is stored in Flash memory, you can use the **microcode reload** command to manually load the new microcode file, and the **configure** command to instruct the system to load the new image automatically at each system boot.

Caution Before you copy a file to Flash, be sure there is ample space available in Flash memory. Compare the size of the file you wish to copy to the amount of available Flash memory shown. If the space available is less than the space required by the file you wish to copy, the copy process will continue, but the entire file will not be copied into Flash.

To compare the size of the microcode image and the amount of Flash memory available, you must know the size of the new microcode image. The image size is specified in the README file that is included on the floppy disk with the new image. Note the size of the new image before proceeding to ensure that you have sufficient available Flash memory for the new image.

Follow these steps to copy a microcode version from the TFTP server to Flash memory:

Step 1 To display the total amount of Flash memory present, its location, any files that currently exist in Flash memory and their size, and the amount of Flash memory remaining, use the **show flash** command. Following is an example of the output that is displayed:

```
Router# show flash

4096K bytes of flash memory on embedded flash (in RP1).

file    offset      length        name
  0     0xD134      55410         sp1-2
  [4085336/4194304 bytes free]
```

Step 2 Compare the amount of available Flash memory (last line in the preceding example) to the size of the new microcode image on the floppy disk to ensure that there is sufficient space available. If you attempt to copy in a new image, and the size of the new image exceeds the available space in Flash, only part of the new image will be copied, and the following error message will be displayed:

```
buffer overflow - xxxx/xxxx
```

where **xxxx/xxxx** is the number of bytes read in/number of bytes available.

Step 3 After you verify that there is sufficient space available in Flash memory for the new image, enter the following command at the privileged-level prompt:

```
Router# copy tftp flash
```

Step 4 Enter the IP address of the remote host:

```
IP address or name of remote host [255.255.255.255]? 1.1.1.106
```

Step 5 Enter the name of the file you want to copy to (*fip10-1* in the following example):

```
Name of file to copy? fip10-1
```

Step 6 To confirm that you want the file copied into Flash, press **Return**.

```
Copy fip10-1 from 1.1.1.106 into flash memory? [confirm]
```

OR

If the correct file is not shown, enter **no** to return to the system prompt and enter the correct file name.

Step 7 If you do not want Flash erased, enter **no** at the next prompt. If you accept the default to erase by pressing Return without first typing **no**, the new image will write over the entire contents of Flash memory and you will lose all other microcode and system software images stored in Flash.

```
Erase flash before writing? [confirm] no
```

While the file is copied to Flash, output similar to the following is displayed:

```
Loading from 1.1.1.106: !!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
 [OK - 108966/4194304 bytes]
Verifying via checksum...
Flash verification successful. Length = 53364, checksum = 0x0000
```

Step 8 To verify that the microcode has been copied to Flash use the **show flash** command. The output should display the file name of the image you copied to Flash (*fip10-1* in the following example):

```
Router# show flash
4096K bytes of flash memory on embedded flash (in RP1).

file   offset    length      name
 0     0x40      55410       sp1-2
 1     0xD0D4    53364       fip10-1
  [4085336/4194304 bytes free]
```

Step 9 To ensure that the new microcode is used when you reboot the system, add the appropriate commands to the configuration file. To modify the configuration file, enter the following command:

```
Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#
```

Step 10 Specify that you are changing the microcode for the FIP (*microcode fip*) and that it will load from Flash memory *(flash)*. Then add the file name of the new microcode image to be loaded from Flash:

```
Router(config)# microcode fip flash fip1-1
```

Step 11 To save the configuration file, press **Ctrl-Z**.

Step 12 Copy the new configuration to NVRAM, as follows:

```
Router# copy running-config startup-config
```

The **microcode reload** command is automatically added to your running configuration. The new FIP microcode image will load automatically the next time the system boots or reinitializes.

Step 13 To load the new microcode immediately, you can instruct the system to load the new microcode by issuing the **microcode reload** configuration command (you must be in configuration mode to enter this command):

```
Router# configure
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# microcode reload
```

Immediately after you enter the **microcode reload** command and press **Return**, the system reloads all microcode. Configuration mode remains enabled; after the reload is complete, press **Ctrl-Z** to exit from configuration mode and return to the system prompt.

Step 14 To verify that the FIP is using the correct microcode, issue the **show configuration** or **show controller cxbus** command. The **show controller cxbus** display indicates the currently loaded and running microcode version for each interface processor.

```
Router# show configuration
```

This completes the procedure for downloading microcode to Flash memory.

Cisco Information Online

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

Available 24 hours a day, 7 days a week, CIO provides a wealth of standard and value-added services to Cisco's customers and business partners. CIO 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.

CIO 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 CIO (called "CIO Classic") supports Zmodem, Kermit, Xmodem, FTP, Internet e-mail, and fax download options, and is excellent for quick access to information over lower bandwidths. The WWW version of CIO provides richly formatted documents with photographs, figures, graphics, and video, as well as hyperlinks to related information.

You can access CIO in the following ways:

- WWW: `http://www.cisco.com`.
- Telnet: `cio.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 CIO's Frequently Asked Questions (FAQ), contact `cio-help@cisco.com`. For additional information, contact `cio-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`.

This document is to be used in conjunction with the *Cisco 7000 Hardware Installation and Maintenance*, *Cisco 7010 Hardware Installation and Maintenance*, *Cisco 7505 Hardware Installation and Maintenance*, *Cisco 7507 Hardware Installation and Maintenance*, and *Cisco 7513 Hardware Installation and Maintenance* publications. (1062fip.fm)