



Cisco 12006 and Cisco 12406 Router Clock and Scheduler, Switch Fabric, and Alarm Card Replacement Instructions

Document Order Number: DOC-78-16106-01, May 30, 2008

Product Numbers: GSR6-CSC=, MAS-GSR6-CSCBLNK=, GSR6-SFC=, GSR6-ALRM=, 12006-CSC=, 12006-SFC=

This publication provides instructions for removing and installing a clock and scheduler card (CSC), switch fabric card (SFC), and alarm card on Cisco 12006 and Cisco 12406 Routers. The CSC and SFC are a card set referred to as the switch fabric. The alarm card is not a part of the switch fabric set.

In addition, instructions for verifying the operation of the system after you replace a card along with switch fabric troubleshooting information are also included.

These two router models are differentiated by the switching capacity of the switch fabric installed in the router:

- Cisco 12006 Router—2.5-Gbps switch fabric
- Cisco 12406 Router—10-Gbps switch fabric

Other than the switch fabric, these routers are identical in most respects. Any differences between the models are described in the appropriate locations. Unless otherwise noted, all information in this publication applies to both router models.



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

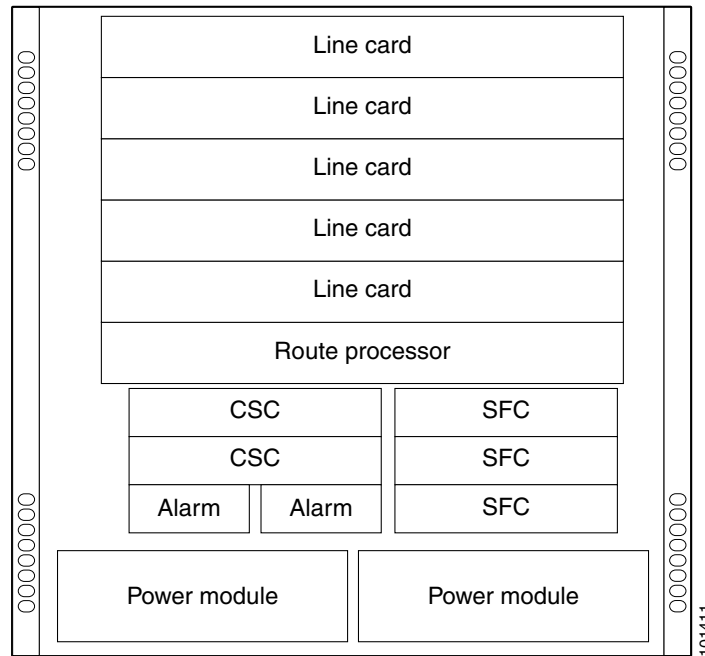
Contents

- [Switch Fabric Overview, page 3](#)
- [Alarm Card Overview, page 4](#)
- [Preparing for Installation, page 4](#)
- [Removing and Installing a CSC or an SFC, page 7](#)
- [Removing and Installing an Alarm Card, page 13](#)
- [Troubleshooting the Switch Fabric, page 15](#)
- [Regulatory, Compliance, and Safety Information, page 20](#)
- [Obtaining Documentation and Submitting a Service Request, page 22](#)

Switch Fabric Overview

The default switch fabric configuration for the Cisco 12006 or Cisco 12406 Router is one CSC and three SFCs. If 2N redundancy is needed, a second CSC can be added to the chassis. The CSC and SFC card slots are located under the route processor (RP) and line card cage. [Figure 1](#) shows the location of these card slots in the chassis.

Figure 1 Cisco 12006 and Cisco 12406 Router Chassis Card Slot Locations



The CSCs occupy the half-width slots on the lower left side of the chassis, directly under the RP and line card cage. The three SFCs occupy the three half-width slots on the lower right side of the chassis. The alarm cards occupy the two narrow slots directly under the CSC slots.

Switch Fabric Types

The Cisco 12006 Router is based on a 2.5-Gbps switch fabric, where each SFC or CSC provides a 2.5-Gbps full-duplex connection to each line card in the system. The 2.5-Gbps switch fabric consists of the 12006 Advanced Clock and Scheduler Card (product number 12006-CSC=) and the 12006 Advanced Switch Fabric Card (product number 12006-SFC=). The 2.5-Gbps switch fabric can be identified by the identification labels on the cards: The CSC is labeled CSC-30/120; the SFC is labeled SFC-30/120.

The Cisco 12406 Router is based on a 10-Gbps switch fabric, where each SFC or CSC provides a 10-Gbps full-duplex connection to each line card in the system. The 10-Gbps switch fabric consists of the Clock and Scheduler Card (product number GSR6-CSC=) and the Switch Fabric Card (product number GSR6-SFC=). The 10-Gbps switch fabric cards are labeled simply CSC and SFC.



Note

You cannot mix 2.5-Gbps switch fabric cards and 10-Gbps switch fabric card types in a chassis. The router will not operate with a mix of switch fabric card types.

Nonredundant and Redundant System Configurations

The Cisco 12006 and Cisco 12406 Routers are available in two system configurations:

1. Nonredundant configuration that includes one CSC and one power module. When you order a Cisco 12006 or Cisco 12406 router, the nonredundant configuration is shipped by default.
2. Redundant configuration that includes two CSCs and two power modules.

For the redundant configuration, EMI compliance and cooling requirements are met by having two CSCs and two power modules installed in the system.

For the nonredundant configuration, EMI compliance and cooling requirements are met only when blank fillers are installed in place of either (or both) the second (unused) CSC slot or the second (unused) power module bay.



Note

When operating your router with a single CSC, the second CSC slot must have a CSC blank filler (MAS-GSR6-CSCBLNK=) installed to ensure EMI compliance.

Alarm Card Overview

The Cisco 12006 and Cisco 12406 Routers are equipped with two alarm cards. These cards are positioned beside one another in two card slots directly below the CSC slots ([Figure 1](#)).



Note

The two alarm cards occupy slots below the two CSC slots in the CSC card cage, but are not part of the switch fabric.

Preparing for Installation

Installation preparation is presented in the following sections:

- [Related Documentation, page 4](#)
- [Tools and Equipment, page 5](#)
- [Safety Guidelines, page 5](#)
- [Preventing Electrostatic Discharge Damage, page 6](#)

Related Documentation

The following Cisco publications contain additional information:

- *Cisco 12006 and Cisco 12406 Router Installation and Configuration Guide*
- *Regulatory Compliance and Safety Information for the Cisco 12000 Series Router*

Tools and Equipment

You will need the following items to remove and install a CSC, an SFC, or an alarm card.

- ESD-preventive strap
- 3/16-inch flat-blade screwdriver

Safety Guidelines

Before you perform any procedure in this publication, review the safety guidelines in this section to avoid injuring yourself or damaging the equipment. In addition, review the safety warnings listed in the *Regulatory Compliance and Safety Information for the Cisco 12000 Series Router* publication (Document Number 78-4347-xx) that accompanied your router before installing, configuring, or maintaining the router.

The following guidelines are for your safety and to protect equipment. The guidelines do not include all hazards. Be alert.

Safety with Equipment

- Always disconnect all power cords and interface cables before moving the system.
- Never assume that power is disconnected from a circuit; always check.
- Keep tools and assembly components away from walkways and equipment rack aisles.
- Do not work alone if potentially hazardous conditions exist.
- 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.

Safety with Electricity

- Before beginning any procedures requiring access to the interior of the router, locate the emergency power-off switch for the room in which you are working.
- Disconnect all power and external cables before installing or removing a router.
- 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.
- Never install equipment that appears damaged.
- Carefully examine your work area for possible hazards such as moist floors, ungrounded power extension cables, and missing safety grounds.
- If an electrical accident does occur, proceed as follows:
 - Use caution; do not become a victim yourself. Disconnect power to the router.
 - If possible, send another person to get medical aid; otherwise, assess the condition of the victim and then call for help.
 - Determine if the person needs rescue breathing or external cardiac compressions; then take appropriate action.

In addition, observe the following guidelines when working with any equipment that is disconnected from a power source but still connected to telephone or network wiring:

- 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

Many router components can be damaged by static electricity. Some components can be damaged by voltages as low as 30V, while static voltages as high as 35,000V can be generated just by handling plastic or foam packing material, or by sliding assemblies across plastic and carpets. Not exercising the proper electrostatic discharge (ESD) precautions can result in intermittent or complete component failures. To minimize the potential for ESD damage, observe the following guidelines:

- Always use an ESD-preventive antistatic wrist strap or ankle strap and ensure that it makes good skin contact.

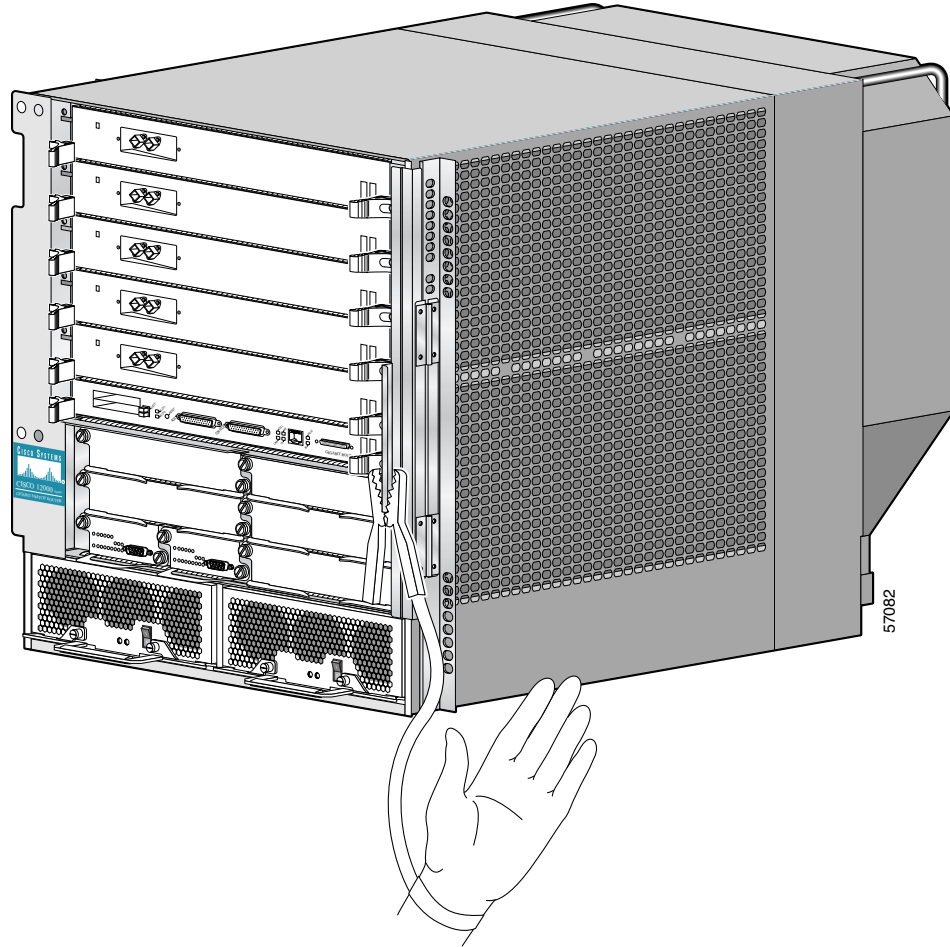


Caution

You should periodically check the resistance value of the ESD-preventive strap. The measurement should be between 1 and 10 megohms.

- When removing or installing a component, make sure the equipment end of your antistatic strap leash is connected to one of the ESD connection sockets on the front of the chassis or to a bare metal surface on the chassis. (See [Figure 2](#).) Avoid contact between the component and your clothing. The ESD-preventive wrist strap only protects the component from ESD voltages on the body; ESD voltages on your clothing can still cause component damage.
- Always place a card component-side-up on an antistatic surface, in an antistatic card rack, or in a static shielding bag. If you are returning the item to the factory, immediately place it in a static shielding bag.
- When installing a line card or route processor (RP), use the ejector levers to seat the card connectors in the backplane, then tighten both captive screws on the faceplate of the card. These screws prevent accidental removal, provide proper grounding for the router, and help to ensure that the card connector is seated in the backplane.
- When removing line cards, clock and scheduler cards, switch fabric cards, or an RP, use the ejector levers to unseat the card connector from the backplane. Pull the metal card carrier out slowly, placing one hand along the bottom of the carrier to guide it straight out of the slot.
- Handle line cards, clock and scheduler cards, switch fabric cards, or an RP by the metal card carrier edges only; avoid touching the board or any connector pins.

Figure 2 Connecting an ESD-preventive Wrist Strap to the Chassis



Removing and Installing a CSC or an SFC

The CSCs occupy the half-width slots on the lower left side of the chassis, under the RP and line card cage. (See [Figure 1](#).) The three SFCs occupy the three half-width slots on the lower right side of the chassis.



Note

When operating your router with a single CSC, the second CSC slot must have a CSC blank filler (MAS-GSR6-CSCBLNK=) installed to ensure EMI compliance.

The CSC blank filler uses the same release levers and captive screws as the CSC, so the blank filler is removed and installed the same way as the CSC. The removal and installation procedures in the following sections apply equally to the CSC blank fillers.

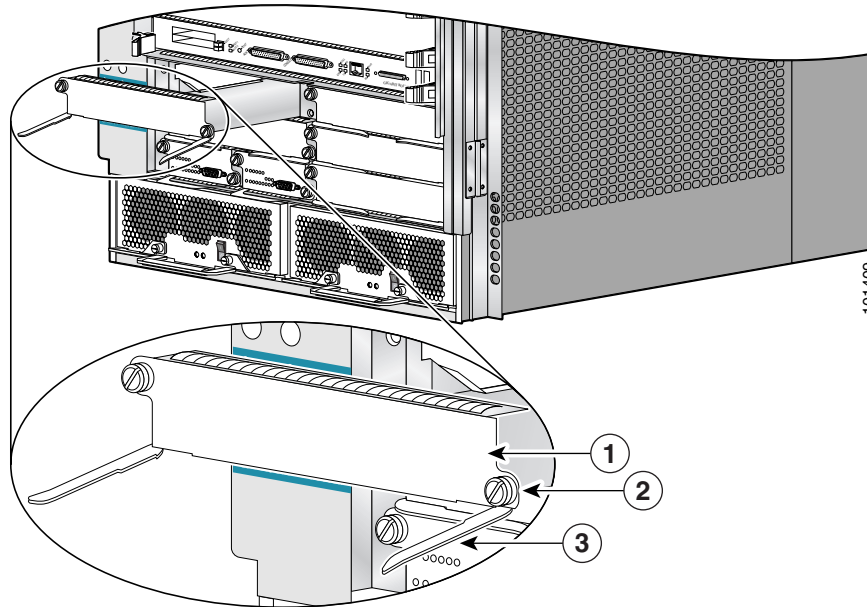
Procedures for removing and installing a CSC or an SFC are described in these sections:

- [Removing and Installing a CSC, page 8](#)
- [Removing and Installing an SFC, page 11](#)

Removing and Installing a CSC

A Cisco 12006 or Cisco 12406 Router configured for redundant CSCs will have two CSCs installed in the two CSC slots; a router configured for nonredundant operation will have one CSC installed in one of the CSC slots, and will have a CSC blank filler installed in the second CSC slot. (See [Figure 1](#).) [Figure 3](#) shows a partially ejected CSC.

Figure 3 Removing and Installing a CSC



1	CSC	3	Ejector lever (2)
2	Captive screw (2)	-	-

Caution

When removing CSCs or CSC blank fillers, remove each component entirely from the chassis and place it in an ESD-safe environment. Do not allow the card or blank to rest partially inserted into the slot, as this will damage the electromagnetic interference (EMI) shielding on the card in the slot directly below.

Caution

Two CSCs (redundant configuration) are required to support CSC online insertion and removal (OIR). This allows you to remove and replace a CSC or an SFC while the system remains powered on. If only one CSC is present, do not remove any cards while the system is powered on.

Procedures for removing and installing a CSC are described in these sections:

- [Removing a CSC, page 9](#)
- [Installing a CSC, page 9](#)
- [Verifying the Installation of the Clock and Scheduler Card, page 10](#)

Removing a CSC

To remove a CSC (or CSC blank filler), see [Figure 3](#) and follow these steps:

-
- Step 1** Attach an ESD-preventive strap to your wrist and connect the leash to the chassis or to another grounded, bare metal surface. (See [Figure 2](#).)
 - Step 2** Loosen the captive screws on each side of the CSC faceplate.
 - Step 3** Grasp the CSC ejector levers and pivot them away from the CSC faceplate.
 - Step 4** Slide the CSC halfway out of the slot, then *stop* sliding.
 - Step 5** Touching only the metal card carrier, use your free hand to support the bottom of the CSC.
 - Step 6** Slide the CSC out of the slot and place it into an antistatic bag or other ESD-preventive container.



Caution

When operating your router with a single CSC, the second CSC slot must have a CSC blank filler (MAS-GSR6-CSCBLNK=) installed to ensure electromagnetic compatibility (EMC) compliance, to avoid overheating, and to ensure compliance with regulatory electromagnetic interference (EMI) standards.

- Step 7** If you plan to return the defective CSC to the factory, repackage it in the shipping container you received with the replacement card.
-

Installing a CSC

To install a CSC (or CSC blank filler), see [Figure 3](#) and follow these steps:

-
- Step 1** Attach an ESD-preventive strap to your wrist and connect the leash to the chassis or to another grounded, bare metal surface. (See [Figure 2](#).)
 - Step 2** Remove the CSC from its antistatic bag or ESD-preventive container.



Caution

Avoid touching the CSC circuitry or any connectors.

- Step 3** Touching only the metal card carrier, use your free hand to support the bottom of the CSC.



Caution

CSC slots are equipped with card alignment grooves on both sides. When you insert a CSC in the slot, make sure you carefully align both edges of the card carrier in the corresponding card slot grooves.

- Step 4** Set both edges of the CSC carrier into the carrier alignment grooves on either side of the CSC card slot.
- Step 5** Pivot the ejector levers away from each other; rotate each ejector lever outward away from the faceplate.
- Step 6** Use both thumbs to slide the card carrier into the CSC slot until both ejector levers make contact with the front of the card cage, then *stop*.
- Step 7** Pivot the ejector levers toward the CSC faceplate until the connector seats in the backplane.


Caution

CSC ejector levers may not fit flush against the CSC faceplate. To ensure that the CSC is properly seated and ensure EMC compliance, tighten the captive screws. Do not overtighten the captive screws; you might strip the threads on the screw or in the insert in the chassis.

Step 8 Tighten the two captive screws.

Verifying the Installation of the Clock and Scheduler Card

To verify router operation after installing a replacement CSC, visually check the LEDs on the two alarm cards. (See [Figure 4](#).) When the system is operating normally, the following LED conditions should be true.

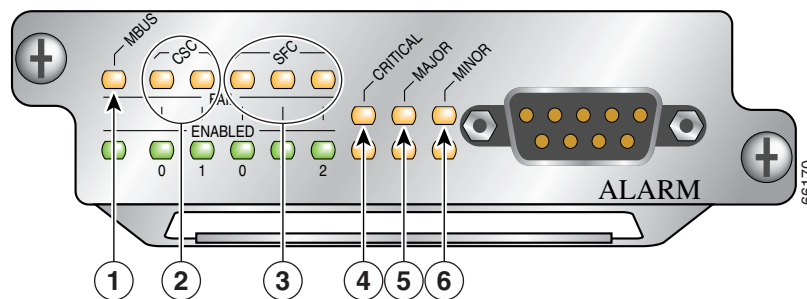
LEDs that normally should be on:

- One MBUS status LED labeled ENABLED
- Two CSC status LEDs labeled ENABLED
- Three SFC status LEDs labeled ENABLED

LEDs that normally should be off:

- One MBUS status LED labeled FAIL
- Two CSC status LEDs labeled FAIL
- Three SFC status LEDs labeled FAIL
- Three router alarm LEDs labeled CRITICAL, MAJOR, MINOR

Figure 4 Alarm Card LEDs On/Off Conditions

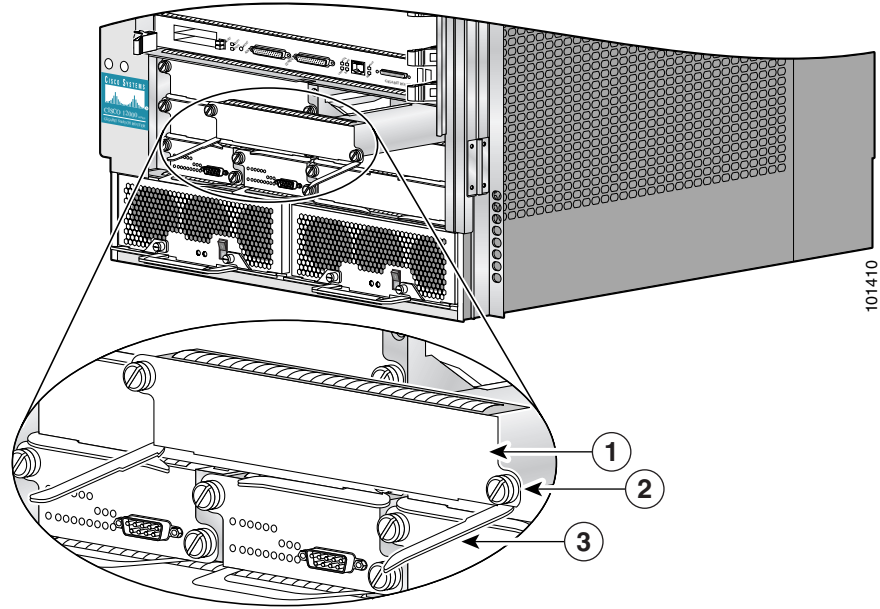


1	MBus status LED	4	Critical alarm LED
2	CSC status LEDs (two)	5	Major alarm LED
3	SFC status LEDs (three)	6	Minor alarm LED

Removing and Installing an SFC

The three SFCs occupy the three half-width slots on the lower right side of the chassis. (See [Figure 1](#).) [Figure 5](#) shows a partially-ejected SFC.

Figure 5 Removing and Installing a Switch Fabric Card



1	SFC	3	Ejector lever (2)
2	Captive screw (2)	–	–

Note

Two CSCs (redundant configuration) are required to support CSC online insertion and removal (OIR). This allows you to remove and replace a CSC or an SFC while the system remains powered on. If only one CSC is present, do not remove any cards while the system is powered on.

Caution

When removing an SFC, remove the card entirely from the chassis and place it in an ESD-safe environment. Do not allow the card to rest partially inserted into the slot, as this damages the EMI shielding on the card in the slot directly below.

Procedures for removing and installing an SFC are described in these sections:

- [Removing an SFC, page 12](#)
- [Installing an SFC, page 12](#)
- [Verifying the Installation of the SFC, page 13](#)

Removing an SFC

To remove an SFC, see [Figure 5](#) and follow these steps:

-
- Step 1** Attach an ESD-preventive strap to your wrist and connect the leash to the chassis or to another grounded, bare metal surface. (See [Figure 2](#).)
 - Step 2** Loosen the captive screw on each side of the SFC faceplate.
 - Step 3** Grasp the card ejector levers and pivot them away from the SFC faceplate.
 - Step 4** Slide the SFC halfway out of the slot, then *stop*.
 - Step 5** Touching only the metal card carrier, use your free hand to support the bottom of the SFC.
 - Step 6** Slide the card out of the slot and place it directly into an antistatic bag or other ESD-preventive container.
 - Step 7** If you plan to return the defective SFC to the factory, repackage it in the shipping container you received with the replacement card.
-

Installing an SFC

To install an SFC, see [Figure 5](#) and follow these steps:

-
- Step 1** Attach an ESD-preventive strap to your wrist and connect the leash to the chassis or to another grounded, bare metal surface. (See [Figure 2](#).)
 - Step 2** Remove the SFC from its antistatic bag or ESD-preventive container.



Caution Avoid touching the SFC circuitry or any connectors.

- Step 3** Touching only the metal card carrier, use your free hand to support the bottom of the SFC.



Caution SFC slots are equipped with card alignment grooves on both sides. When you insert a SFC in the slot, make sure you carefully align both edges of the card carrier in the corresponding card slot grooves.

- Step 4** Set both edges of the SFC carrier into the carrier alignment grooves on either side of the SFC slot.
- Step 5** Pivot the ejector levers away from each other; rotate each ejector lever outward away from the faceplate.
- Step 6** Use both thumbs to slide the card carrier into the SFC slot until both ejector levers make contact with the front of the card cage, then *stop*.
- Step 7** Pivot the ejector levers toward the faceplate until the connector seats in the backplane.



Caution SFC ejector levers may not fit flush against the SFC faceplate. To ensure that the SFC is properly seated and ensure EMC compliance, tighten the captive screws. Do not overtighten the captive screws; you might strip the threads on the screw or in the insert in the chassis.

- Step 8** Tighten the captive screws on each side of the SFC faceplate.
-

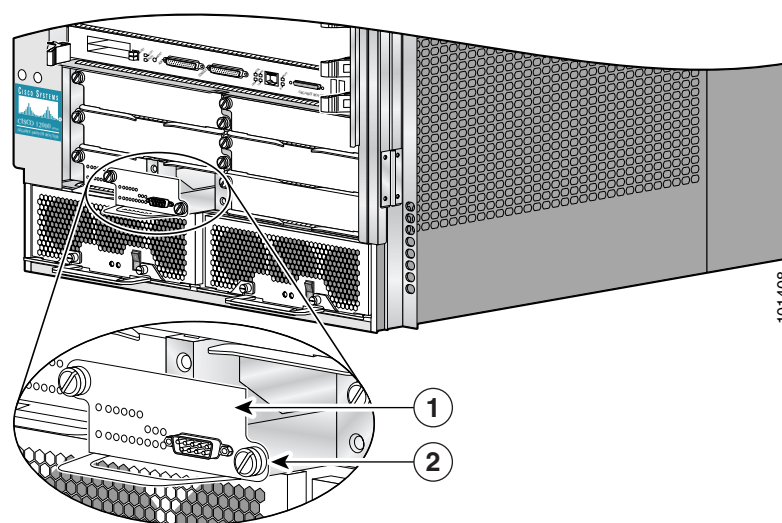
Verifying the Installation of the SFC

To verify router operation after installing a replacement SFC, see the “[Verifying the Installation of the Clock and Scheduler Card](#)” section on page 10. The description of the alarm card LEDs applies equally to checking SFC operation.

Removing and Installing an Alarm Card

The two alarm cards occupy the card slots in the alarm card bay. These slots are located on the bottom left side of the chassis, directly underneath the CSC slots. (See [Figure 1](#).) [Figure 6](#) shows a partially-ejected alarm card.

Figure 6 Removing and Installing an Alarm Card



1	Alarm card	2	Captive screw (2)
---	------------	---	-------------------



Note

Alarm cards support online insertion and removal (OIR), so you can remove and replace an alarm card while the system remains powered on.

Procedures for removing and installing an alarm card are described in the following sections:

- [Removing an Alarm Card](#), page 14
- [Installing an Alarm Card](#), page 14
- [Verifying the Installation of the Alarm Card](#), page 14

Removing an Alarm Card

To remove an alarm card, see [Figure 6](#) and follow these steps:

-
- Step 1** Attach an ESD-preventive strap to your wrist and connect the leash to the chassis or to another grounded, bare metal surface. (See [Figure 2](#).)
 - Step 2** Loosen the two captive screw on each side of the alarm card.
 - Step 3** Grasp the handle on the front of the alarm card and slide the alarm card halfway out of the slot, then *stop*.
 - Step 4** Touching only the metal card carrier, use your free hand to support the bottom of the alarm card.
 - Step 5** Remove the card from the slot and place it into an antistatic bag or other ESD-preventive container.
 - Step 6** If you plan to return the defective alarm card to the factory, repackage it in the shipping container you received with the replacement card.
-

Installing an Alarm Card

To install an alarm card, see [Figure 6](#) and follow these steps:

-
- Step 1** Attach an ESD-preventive strap to your wrist and connect the leash to the chassis or to another grounded, bare metal surface. (See [Figure 2](#).)
 - Step 2** Remove the alarm card from its antistatic bag or ESD-preventive container.



Caution Avoid touching the card circuitry or any connectors.

- Step 3** Touching only the handle, use your free hand to support the bottom of the alarm card.
- Step 4** Slide the alarm card into the alarm card slot until it contacts the backplane, then *stop*.
- Step 5** Use both thumbs to push the card carrier into the slot until the alarm card connector seats itself against the backplane connector.



Caution Alarm card captive screws must be tightened to ensure EMC compliance. Do not overtighten the captive screws; you might strip the threads on the screw or in the insert in the alarm card faceplate.

- Step 6** Tighten the two captive screws to secure the alarm card in the chassis.
-

Verifying the Installation of the Alarm Card

To verify router operation after installing a replacement alarm card, see the [“Verifying the Installation of the Clock and Scheduler Card”](#) section on page 10. The description of the alarm card LEDs applies equally to checking alarm card operation.

Troubleshooting the Switch Fabric

This section describes the procedures needed to troubleshoot problems with the switch fabric. The RP and the line cards connect through the crossbar switch fabric, which provides a high-speed physical path for most inter-card communication. Among the messages passed between the RP and the line cards over the switch fabric are, actual packets being routed and received, forwarding information, traffic statistics, and most management and control information. This information is useful in diagnosing hardware-related failures.



Note

This section is recommended only for advanced Cisco IOS software operators and system administration personnel. Refer to the appropriate Cisco IOS software publications for detailed Cisco IOS information.

To troubleshoot the switch fabric, follow these steps:

Step 1 Collect the needed data from the RPs and line cards.



Note

When you connect to the line card, use the **attach** command. The **execute-on** command is dependent upon the inter-process communication (IPC) which operates over the switch fabric. If you are having problems with IPC, the commands that run remotely through the switch fabric can time out. The **attach <slot #>** command travels over the MBus and not the IPC.

Step 2 Use the **show controllers fia** command on the primary and secondary RPs and save the output.

Step 3 Use the **attach <slot #>** command to access a line card.

Step 4 Use the **show controllers fia** command on all installed line cards and save the output from each.

Step 5 Gather the output and proceed to the [Analyzing the Data](#) section.

Analyzing the Data

Switch fabric problems can occur due to failures in any of the following components:

- RP
- Line card hardware
- Backplane
- CSCs/SFCs

When troubleshooting switch fabric errors, you need to look for patterns with regard to which components are reporting errors. For example, if you combine the **show controllers fia** output from all the RPs and line cards, you can determine if there is an error pattern. The following subsections discuss the values within the output that can help you determine any error patterns.



Note

The sample output in this section comes from a Cisco 12016 router.

crc16 Output

The `crc16` data line from the `show controllers fia` command is an important indicator of hardware problems. If one line card or one CSC/SFC has been on line inserted and removed, you can expect to see some `crc16` error data. However, this number should not continue to increase. If the number is increasing, you might need to replace some faulty hardware. It is very important to correlate the data from both the primary RP and the secondary RP and all installed line cards. The example output below shows the status of the primary RP. The `crc16` data line is underlined and is showing errors from `sfc1`.

```
Router#show controllers fia
Fabric configuration: Full bandwidth, redundant fabric
Master Scheduler: Slot 17 Backup Scheduler: Slot 16
From Fabric FIA Errors
-----
redund fifo parity 0      redund overflow 0      cell drops 0
crc32 lkup parity 0      cell parity 0      crc32 0
Switch cards present 0x001F Slots 16 17 18 19 20
Switch cards monitored 0x001F Slots 16 17 18 19 20
Slot: 16 17 18 19 20
Name: csc0 csc1 sfc0 sfc1 sfc2
-----
los 0 0 0 0 0
state Off Off Off Off Off
crc16 0 0 0 1345 0
To Fabric FIA Errors
-----
sca not pres 0      req error 0      uni FIFO overflow 0
grant parity 0      multi req 0      uni FIFO undrflow 0
cntrl parity 0      uni req 0      crc32 lkup parity 0
multi FIFO 0      empty dst req 0      handshake error 0
cell parity 0
```

In the example output below, you can see the status of the line card in slot 2. The `crc16` data line is underlined and is showing errors from `sfc1`. Remember to use the `attach` command and not the `execute-on` command to access the line cards.

```
Router#attach 2
Entering Console for 4 port ATM Over SONET OC-3c/STM-1 in Slot: 2
Type "exit" to end this session
Press RETURN to get started!
LC-Slot2>
LC-Slot2>enable
LC-Slot2#show controllers fia
From Fabric FIA Errors
-----
redund FIFO parity 0      redund overflow 0      cell drops 0
crc32 lkup parity 0      cell parity 0      crc32 0
Switch cards present 0x001F Slots 16 17 18 19 20
Switch cards monitored 0x001F Slots 16 17 18 19 20
Slot: 16 17 18 19 20
Name: csc0 csc1 sfc0 sfc1 sfc2
-----
Los 0 0 0 0 0
state Off Off Off Off Off
crc16 0 0 0 1345 0
To Fabric FIA Errors
-----
sca not pres 0      req error 0      uni fifo overflow 0
grant parity 0      multi req 0      uni fifo undrflow 0
cntrl parity 0      uni req 0      crc32 lkup parity 0
multi fifo 0      empty DST req 0      handshake error 0
cell parity 0
```

```

LC-Slot2#exit
Disconnecting from slot 2.
Connection Duration: 00:00:21
Router#

```

Once you have gathered the **show controllers fia** command data from the RPs and line cards, you can create a table similar to [Table 1](#).

Table 1 Error Data Collection Table

Card Slot	CSC 0	CSC 1	SFC 0	SFC 1	SFC 2
0				ERROR	
1					
2				ERROR	
3				ERROR	
4					
5				ERROR	

This table indicates that more than one line card is reporting errors coming from SFC 1. Therefore, the first step is to change this SFC. Whenever a replacement is recommended, first verify that the card is correctly seated. You should ALWAYS reseal the corresponding card to be sure it is correctly seated. If, after reseating the card, the CRCs are still increasing, then go ahead and replace the part. See the [“Properly Seating Switch Fabric Cards”](#) section on page 18.

The common failure patterns and recommended actions for crc16 errors are as follows (one step at a time until the problem goes away):

1. Errors indicated on more than one line card from the same switch fabric card:
 - a. Replace the switch fabric card in the slot corresponding to the errors
 - b. Replace all switch fabric cards
 - c. Replace the backplane
2. Errors indicated on one line card from more than one switch fabric card:
 - a. Replace the line card
 - b. If errors are incrementing, replace the current master CSC
 - c. If errors are not incrementing and the current master is CSC0, replace CSC1

Grant Parity and Request Errors

Another troubleshooting indicator comes from the console logs or the output of the **show log** command, in the form of grant parity and request errors. Look for the following type of message that indicates a grant parity error:

```

%FABRIC-3-PARITYERR: To Fabric parity error was detected.
Grant parity error Data = 0x2.
SLOT 1:%FABRIC-3-PARITYERR: To Fabric parity error was detected.
Grant parity error Data = 0x1

```

You can also use the output from the **show controllers fia** command. Important information is underlined:

```

Router#show controllers fia

```

Fabric configuration: Full bandwidth, redundant fabric
Master Scheduler: Slot 17 Backup Scheduler: Slot 16

From Fabric FIA Errors

redund FIFO parity 0 redund overflow 0 cell drops 76

```
crc32 lkup parity 0    cell parity 0    crc32 0
Switch cards present  0x001F    Slots  16 17 18 19 20
Switch cards monitored 0x001F    Slots  16 17 18 19 20
Slot:      16      17      18      19      20
Name:     csc0     csc1     sfc0     sfc1     sfc2
-----
Los       0        0        0        0        0
state    Off      Off      Off      Off      Off
crc16    876      257      876      876      876
```

To Fabric FIA Errors

```
-----
sca not pres 0          req error 1          uni fifo overflow 0
grant parity 1        multi req 0          uni fifo undrflow 0

cntrl parity 0          uni req 0          crc32 lkup parity 0
multi fifo 0           empty DST req 0    handshake error 0
cell parity 0
```

The common failure patterns and recommended actions for grant parity and request errors are as follows (one step at a time until the problem goes away):

1. Grant errors on more than one line card:
 - a. Replace the CSC (see the note below to know which one should be swapped)
 - b. Replace the backplane
2. Grant errors on one line card:
 - a. Replace the line card
 - a. Replace the CSC (see the note below to know which one should be swapped)
 - b. Replace the backplane



Note

If multiple line cards are reporting grant parity or request errors and the router is still functioning, then a CSC switchover has occurred. The failed CSC is the one that is currently the backup CSC (not the one listed as “Master Scheduler” in the **show controllers fia** output). If “Halted” is next to the heading “From Fabric FIA Errors” or “To Fabric FIA Errors,” or if the router is no longer forwarding traffic, then a CSC switchover has not occurred and the failing CSC is the one listed as “Master Scheduler.” By default, the CSC in slot 17 is the primary and the CSC in slot 16 is the backup.

Properly Seating Switch Fabric Cards

The switch fabric cards in the router can be challenging to insert, and may require a small amount of force to seat correctly. If either of the CSCs are not seated properly, you may see the following error message:

```
%MBUS-0-NOCS: Must have at least 1 CSC card in slot 16 or 17
```

%MBUS-0-FABINIT: Failed to initialize switch fabric infrastructure



Note

You may also get this error message if there are only enough CSCs and SFCs seated for quarter bandwidth configurations. Quarter bandwidth configurations are no longer supported on Cisco 12000 Series routers.

When dealing with switch fabric and line card booting problems, it is important to verify that all CSCs and SFCs are correctly seated and powered on. The output from the **show version** and **show controllers fia** commands tells you which hardware configuration is currently running on the box. Important data is underlined.

```
Router#show version
Cisco Internetwork Operating System Software
IOS (tm) GS Software (GSR-P-M), Experimental Version 12.0(20010505:112551)
Copyright (c) 1986-2001 by cisco Systems, Inc.
Compiled Mon 14-May-01 19:25 by tmcclure
Image text-base: 0x60010950, data-base: 0x61BE6000

ROM: System Bootstrap, Version 11.2(17)GS2, [htseng 180]
EARLY DEPLOYMENT RELEASE SOFTWARE (fc1)
BOOTFLASH: GS Software (GSR-BOOT-M), Version 12.0(15.6)S,
EARLY DEPLOYMENT MAINTENANCE INTERIM SOFTWARE

Router uptime is 17 hours, 53 minutes
System returned to ROM by reload at 23:59:40 MET Mon Jul 2 2001
System restarted at 00:01:30 MET Tue Jul 3 2001
System image file is "tftp://172.17.247.195/gsr-p-mz.15S2plus-FT-14-May-2001"

cisco 12016/GRP (R5000) processor (revision 0x01) with 262144K bytes of memory.
R5000 CPU at 200Mhz, Implementation 35, Rev 2.1, 512KB L2 Cache
Last reset from power-on

2 Route Processor Cards
1 Clock Scheduler Card
3 Switch Fabric Cards
1 8-port OC3 POS controller (8 POs).
1 OC12 POS controller (1 POs).
1 OC48 POS E.D. controller (1 POs).
7 OC48 POS controllers (7 POs).
1 Ethernet/IEEE 802.3 interface(s)
17 Packet over SONET network interface(s)
507K bytes of non-volatile configuration memory.

20480K bytes of Flash PCMCIA card at slot 0 (Sector size 128K).
8192K bytes of Flash internal SIMM (Sector size 256K).

Router#show controller fia
Fabric configuration: Full bandwidth nonredundant
Master Scheduler: Slot 17
```

Additional troubleshooting information is available on Cisco.com.

Regulatory, Compliance, and Safety Information

This section includes regulatory, compliance, and safety information in the following sections:

- [Translated Safety Warnings and Agency Approvals](#)
- [Electromagnetic Compatibility Regulatory Statements](#)

Translated Safety Warnings and Agency Approvals

The complete list of translated safety warnings and agency approvals is available in the *Regulatory Compliance and Safety Information for Cisco 12000 Series Routers* publication (Document Number 78-4347-xx).

Electromagnetic Compatibility Regulatory Statements

FCC Class A Compliance

This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to part 15 of the FCC rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio-frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference, in which case users will be required to correct the interference at their own expense.

Modifying the equipment without Cisco's authorization may result in the equipment no longer complying with FCC requirements for Class A digital devices. In that event, your right to use the equipment may be limited by FCC regulation and you may be required to correct any interference to radio or television communication at your own expense.

You can determine whether your equipment is causing interference by turning it off. If the interference stops, it was probably caused by the Cisco equipment or one of its peripheral devices. If the equipment causes interference to radio or television reception, try to correct the interference by using one or more of the following measures:

- Turn the television or radio antenna until the interference stops.
- Move the equipment to one side or the other of the television or radio.
- Move the equipment farther away from the television or radio.
- Plug the equipment into an outlet that is on a different circuit from the television or radio. (That is, make certain the equipment and the television or radio are on circuits controlled by different circuit breakers or fuses.)

CISPR 22

This apparatus complies with CISPR 22/EN55022 Class B radiated and conducted emissions requirements.

Canada

English Statement of Compliance

This class A digital apparatus complies with Canadian ICES-003.

French Statement of Compliance

Cet appareil numérique de la classe A est conforme à la norme NMB-003 du Canada.

Europe (EU)

This apparatus complies with EN55022 Class B and EN55024 standards when used as ITE/TTE equipment, and EN300386 for Telecommunications Network Equipment (TNE) in both installation environments, telecommunication centers and other indoor locations.

VCCI Class A Notice for Japan



Warning

This is a Class A product based on the standard of the Voluntary Control Council for Interference by Information Technology Equipment (VCCI). If this equipment is used in a domestic environment, radio disturbance may arise. When such trouble occurs, the user may be required to take corrective actions. Statement 191

警告 これは、情報処理装置等電波障害自主規制協議会（VCCI）の規定に基づくクラスA装置です。この装置を家庭環境で使用すると、電波妨害を引き起こすことがあります。この場合には、使用者が適切な対策を取るようにより要求されることがあります。

Class A Notice for Hungary



Warning

This equipment is a class A product and should be used and installed properly according to the Hungarian EMC Class A requirements (MSZEN55022). Class A equipment is designed for typical commercial establishments for which special conditions of installation and protection distance are used. Statement 256

Figyelmeztetés a felhasználói kézikönyv számára: Ez a berendezés "A" osztályú termék, felhasználására és üzembe helyezésére a magyar EMC "A" osztályú követelményeknek (MSZ EN 55022) megfelelően kerülhet sor, illetve ezen "A" osztályú berendezések csak megfelelő kereskedelmi forrásból származhatnak, amelyek biztosítják a megfelelő speciális üzembe helyezési körülményeket és biztonságos üzemelési távolságok alkalmazását.

Class A Notice for Taiwan and Other Traditional Chinese Markets



Warning

This is a Class A Information Product, when used in residential environment, it may cause radio frequency interference, under such circumstances, the user may be requested to take appropriate countermeasures. Statement 257

警告 這是甲類資訊產品，在居住環境中使用時，可能會造成射頻干擾，在這種情況下，使用者會被要求採取某些適當的對策。

Class A Notice for Korea



Warning

This is a Class A Device and is registered for EMC requirements for industrial use. The seller or buyer should be aware of this. If this type was sold or purchased by mistake, it should be replaced with a residential-use type. Statement 294

주의 A급 기기 이 기기는 업무용으로 전자파 적합 등록을 한 기기이
오니 판매자 또는 사용자는 이 점을 주의하시기 바라며 만약
잘못 판매 또는 구입하였을 때에는 가정용으로 교환하시기 바랍니다.

Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, submitting a service request, and gathering additional information, see the monthly *What's New in Cisco Product Documentation*, which also lists all new and revised Cisco technical documentation, at:

<http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html>

Subscribe to the *What's New in Cisco Product Documentation* as a Really Simple Syndication (RSS) feed and set content to be delivered directly to your desktop using a reader application. The RSS feeds are a free service and Cisco currently supports RSS version 2.0.

This document is to be used in conjunction with the *Cisco 12006 and Cisco 12406 Router Installation and Configuration Guide*.

CCDE, CCENT, Cisco Eos, Cisco Lumin, Cisco Nexus, Cisco StadiumVision, the Cisco logo, DCE, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn is a service mark; and Access Registrar, Aironet, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, CCVP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, EtherFast, EtherSwitch, Event Center, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, iQuick Study, IronPort, the IronPort logo, LightStream, Linksys, MediaTone, MeetingPlace, MGX, Networkers, Networking Academy, Network Registrar, PCNow, PIX, PowerPanels, ProConnect, ScriptShare, SenderBase, SMARTnet, Spectrum Expert, StackWise, The Fastest Way to Increase Your Internet Quotient, TransPath, WebEx, and the WebEx logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0805R)

Copyright © 2008 Cisco Systems, Inc. All rights reserved.