



Cisco FlexWAN and Enhanced FlexWAN Modules Installation Guide

January 2009

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
<http://www.cisco.com>
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

Text Part Number: OL-8357-01

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The following information is for FCC compliance of Class A devices: 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.

The following information is for FCC compliance of Class B devices: The equipment described in this manual generates and may radiate radio-frequency energy. If it is not installed in accordance with Cisco's installation instructions, it may cause interference with radio and television reception. This equipment has been tested and found to comply with the limits for a Class B digital device in accordance with the specifications in part 15 of the FCC rules. These specifications are designed to provide reasonable protection against such interference in a residential installation. However, there is no guarantee that interference will not occur in a particular installation.

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

Modifications to this product not authorized by Cisco Systems, Inc. could void the FCC approval and negate your authority to operate the product.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES

CCDE, CCENT, Cisco Eos, Cisco Lumin, Cisco Nexus, Cisco StadiumVision, Cisco TelePresence, Cisco WebEx, the Cisco logo, DCE, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn and Cisco Store are service marks; 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, iQuick Study, IronPort, the IronPort logo, LightStream, Linksys, MediaTone, MeetingPlace, MeetingPlace Chime Sound, 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. (0809R)

Cisco FlexWAN and Enhanced FlexWAN Modules Installation Guide
Copyright © 2008, Cisco Systems, Inc.
All rights reserved.

Cisco FlexWAN and Enhanced FlexWAN Modules Installation Guide
© 2005 Cisco Systems, Inc. All rights reserved.



CONTENTS

Preface	v
Document Revision History	v
Audience	v
Organization	vi
Related Documentation	vi
Obtaining Documentation	vii
Cisco.com	vii
Product Documentation DVD	vii
Ordering Documentation	vii
Documentation Feedback	viii
Cisco Product Security Overview	viii
Reporting Security Problems in Cisco Products	viii
Obtaining Technical Assistance	ix
Cisco Technical Support & Documentation Website	ix
Submitting a Service Request	x
Definitions of Service Request Severity	x
Obtaining Additional Publications and Information	xi
CHAPTER 1	
Installing the FlexWAN and Enhanced FlexWAN Modules	1-1
Preparing to Install the FlexWAN or Enhanced FlexWAN Module	1-1
Preventing Electrostatic Discharge Damage	1-1
Installing the FlexWAN and Enhanced FlexWAN Modules	1-3
Installing a FlexWAN or Enhanced FlexWAN Module Port Adapter	1-6
Required Tools and Equipment	1-6
Handling Port Adapters	1-7
Replacing Port Adapters	1-7
Installing a New Port Adapter in an Enhanced FlexWAN Module	1-8
Warnings and Cautions	1-9

CHAPTER 2

Replacing or Upgrading Module Memory 2-1

Notes and Cautions 2-1

Removing SODIMMs 2-2

Installing New SODIMMs 2-4

Checking an SDRAM Upgrade or Replacement 2-5

CHAPTER 3

CLI Commands for the FlexWAN and Enhanced FlexWAN Modules 3-1

INDEX



Preface

This guide provides installation procedures for the FlexWAN module (WS-X6182-2PA) and the fabric-enabled Enhanced FlexWAN module (WS-X6582-2PA). This preface contains these sections:

- [Document Revision History, page 5](#)
- [Audience, page 5](#)
- [Organization, page 6](#)
- [Related Documentation, page 6](#)
- [Obtaining Documentation, page 7](#)
- [Obtaining Documentation and Submitting a Service Request, page 9](#)
- [Cisco Product Security Overview, page 8](#)
- [Obtaining Technical Assistance, page 9](#)
- [Obtaining Additional Publications and Information, page 10](#)

Document Revision History

The Document Revision History table below records technical changes to this document. The table shows the document revision number for the change, the date of the change, and a brief summary of the change.

Revision	Date	Change Summary
OL-83547-01	September 2005	This is the initial release of this document.

Audience

This publication is for experienced network administrators who are responsible for configuring and maintaining the FlexWAN and Enhanced FlexWAN modules for the Cisco 7600 series router and Catalyst 6500 series switch.

Only trained and qualified service personnel (as defined in IEC 60950 and AS/NZS3260) should install, replace, or service the equipment described in this publication.

Organization

This publication is organized as follows:

Chapter	Title	Description
Chapter 1	Installing the FlexWAN and Enhanced FlexWAN Modules	Provides the procedures for installing the FlexWAN and Enhanced FlexWAN modules. This chapter also describes how to install and replace port adapters.
Chapter 2	Replacing or Upgrading Module Memory	This chapter describes the procedure for removing and replacing the memory modules (SODIMMs) on the FlexWAN module in the Catalyst 6500 series switches or Cisco 7600 series routers.
Chapter 3	CLI Commands for the FlexWAN and Enhanced FlexWAN Modules	Describes the CLI commands for displaying FlexWAN or Enhanced FlexWAN module status, configuration, and statistical information, as well as the commands for debugging purposes.

Related Documentation

The following related publications are available:

- *Regulatory Compliance and Safety Information for the Cisco 7600 Series Routers*
- *Cisco 7600 Series Router Installation Guide*
- *Cisco 7609 Router Installation Guide*
- *Cisco 7600 Series Router Module Installation Guide*
- *Cisco 7600 Series Router Software Configuration Guide*
- *Cisco 7600 Series Cisco IOS Command Reference*
- *Cisco 7600 Series Cisco IOS System Message Guide*
- *Cisco 7600 Series Cisco IOS Software Configuration Guide*
- *Cisco 7600 Series Routers Documentation Roadmap*
- *Regulatory Compliance and Safety Information for the Catalyst 6500 Series Switches*
- *Site Preparation and Safety Guide*
- *Catalyst 6500 Series Switch Module Guide*
- *Catalyst 6500 Series Switch Installation Guide*
- *Catalyst 6500 Series Software Configuration Guide*
- *Catalyst 6500 Series Command Reference*
- *Catalyst 6500 Series Cisco IOS Software Configuration Guide*
- *Catalyst 6500 Series Cisco IOS Command Reference*
- *ATM Configuration and Command Reference—Catalyst 5000 and 6000 Family Switches*
- *Catalyst 6500 Series System Message Guide*

For information about MIBs, refer to this URL:

<http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml>

Obtaining Documentation

Cisco documentation and additional literature are available on Cisco.com. Cisco also provides several ways to obtain technical assistance and other technical resources. These sections explain how to obtain technical information from Cisco Systems.

Cisco.com

You can access the most current Cisco documentation at this URL:

<http://www.cisco.com/techsupport>

You can access the Cisco website at this URL:

<http://www.cisco.com>

You can access international Cisco websites at this URL:

http://www.cisco.com/public/countries_languages.shtml

Product Documentation DVD

Cisco documentation and additional literature are available in the Product Documentation DVD package, which may have shipped with your product. The Product Documentation DVD is updated regularly and may be more current than printed documentation.

The Product Documentation DVD is a comprehensive library of technical product documentation on portable media. The DVD enables you to access multiple versions of hardware and software installation, configuration, and command guides for Cisco products and to view technical documentation in HTML. With the DVD, you have access to the same documentation that is found on the Cisco website without being connected to the Internet. Certain products also have .pdf versions of the documentation available.

The Product Documentation DVD is available as a single unit or as a subscription. Registered Cisco.com users (Cisco direct customers) can order a Product Documentation DVD (product number DOC-DOCDVD=) from Cisco Marketplace at this URL:

<http://www.cisco.com/go/marketplace/>

Ordering Documentation

Beginning June 30, 2005, registered Cisco.com users may order Cisco documentation at the Product Documentation Store in the Cisco Marketplace at this URL:

<http://www.cisco.com/go/marketplace/>

Nonregistered Cisco.com users can order technical documentation from 8:00 a.m. to 5:00 p.m. (0800 to 1700) PDT by calling 1 866 463-3487 in the United States and Canada, or elsewhere by calling 011 408 519-5055. You can also order documentation by e-mail at tech-doc-store-mkpl@external.cisco.com or by fax at 1 408 519-5001 in the United States and Canada, or elsewhere at 011 408 519-5001.

Cisco Product Security Overview

Cisco provides a free online Security Vulnerability Policy portal at this URL:

http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html

From this site, you can perform these tasks:

- Report security vulnerabilities in Cisco products.
- Obtain assistance with security incidents that involve Cisco products.
- Register to receive security information from Cisco.

A current list of security advisories and notices for Cisco products is available at this URL:

<http://www.cisco.com/go/psirt>

If you prefer to see advisories and notices as they are updated in real time, you can access a Product Security Incident Response Team Really Simple Syndication (PSIRT RSS) feed from this URL:

http://www.cisco.com/en/US/products/products_psirt_rss_feed.html

Reporting Security Problems in Cisco Products

Cisco is committed to delivering secure products. We test our products internally before we release them, and we strive to correct all vulnerabilities quickly. If you think that you might have identified a vulnerability in a Cisco product, contact PSIRT:

- Emergencies—security-alert@cisco.com

An emergency is either a condition in which a system is under active attack or a condition for which a severe and urgent security vulnerability should be reported. All other conditions are considered nonemergencies.

- Nonemergencies—psirt@cisco.com

In an emergency, you can also reach PSIRT by telephone:

- 1 877 228-7302
- 1 408 525-6532



Tip

We encourage you to use Pretty Good Privacy (PGP) or a compatible product to encrypt any sensitive information that you send to Cisco. PSIRT can work from encrypted information that is compatible with PGP versions 2.x through 8.x.

Never use a revoked or an expired encryption key. The correct public key to use in your correspondence with PSIRT is the one linked in the Contact Summary section of the Security Vulnerability Policy page at this URL:

http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html

The link on this page has the current PGP key ID in use.

Obtaining Technical Assistance

Cisco Technical Support provides 24-hour-a-day award-winning technical assistance. The Cisco Technical Support & Documentation website on Cisco.com features extensive online support resources. In addition, if you have a valid Cisco service contract, Cisco Technical Assistance Center (TAC) engineers provide telephone support. If you do not have a valid Cisco service contract, contact your reseller.

Cisco Technical Support & Documentation Website

The Cisco Technical Support & Documentation website provides online documents and tools for troubleshooting and resolving technical issues with Cisco products and technologies. The website is available 24 hours a day, at this URL:

<http://www.cisco.com/techsupport>

Access to all tools on the Cisco Technical Support & Documentation website requires a Cisco.com user ID and password. If you have a valid service contract but do not have a user ID or password, you can register at this URL:

<http://tools.cisco.com/RPF/register/register.do>



Note

Use the Cisco Product Identification (CPI) tool to locate your product serial number before submitting a web or phone request for service. You can access the CPI tool from the Cisco Technical Support & Documentation website by clicking the **Tools & Resources** link under Documentation & Tools. Choose **Cisco Product Identification Tool** from the Alphabetical Index drop-down list, or click the **Cisco Product Identification Tool** link under Alerts & RMAs. The CPI tool offers three search options: by product ID or model name; by tree view; or for certain products, by copying and pasting **show** command output. Search results show an illustration of your product with the serial number label location highlighted. Locate the serial number label on your product and record the information before placing a service call.

Submitting a Service Request

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.

Definitions of Service Request Severity

To ensure that all service requests are reported in a standard format, Cisco has established severity definitions.

Severity 1 (S1)—Your network is “down,” or there is a critical impact to your business operations. You and Cisco will commit all necessary resources around the clock to resolve the situation.

Severity 2 (S2)—Operation of an existing network is severely degraded, or significant aspects of your business operation are negatively affected by inadequate performance of Cisco products. You and Cisco will commit full-time resources during normal business hours to resolve the situation.

Severity 3 (S3)—Operational performance of your network is impaired, but most business operations remain functional. You and Cisco will commit resources during normal business hours to restore service to satisfactory levels.

Severity 4 (S4)—You require information or assistance with Cisco product capabilities, installation, or configuration. There is little or no effect on your business operations.

Obtaining Additional Publications and Information

Information about Cisco products, technologies, and network solutions is available from various online and printed sources.

- Cisco Marketplace provides a variety of Cisco books, reference guides, documentation, and logo merchandise. Visit Cisco Marketplace, the company store, at this URL:

<http://www.cisco.com/go/marketplace/>

- *Cisco Press* publishes a wide range of general networking, training and certification titles. Both new and experienced users will benefit from these publications. For current Cisco Press titles and other information, go to Cisco Press at this URL:

<http://www.ciscopress.com>

- *Packet* magazine is the Cisco Systems technical user magazine for maximizing Internet and networking investments. Each quarter, Packet delivers coverage of the latest industry trends, technology breakthroughs, and Cisco products and solutions, as well as network deployment and troubleshooting tips, configuration examples, customer case studies, certification and training information, and links to scores of in-depth online resources. You can access Packet magazine at this URL:

<http://www.cisco.com/packet>

- *iQ Magazine* is the quarterly publication from Cisco Systems designed to help growing companies learn how they can use technology to increase revenue, streamline their business, and expand services. The publication identifies the challenges facing these companies and the technologies to help solve them, using real-world case studies and business strategies to help readers make sound technology investment decisions. You can access iQ Magazine at this URL:

<http://www.cisco.com/go/iqmagazine>

or view the digital edition at this URL:

<http://ciscoiq.texterity.com/ciscoiq/sample/>

- *Internet Protocol Journal* is a quarterly journal published by Cisco Systems for engineering professionals involved in designing, developing, and operating public and private internets and intranets. You can access the Internet Protocol Journal at this URL:
<http://www.cisco.com/ipj>
- Networking products offered by Cisco Systems, as well as customer support services, can be obtained at this URL:
<http://www.cisco.com/en/US/products/index.html>
- Networking Professionals Connection is an interactive website for networking professionals to share questions, suggestions, and information about networking products and technologies with Cisco experts and other networking professionals. Join a discussion at this URL:
<http://www.cisco.com/discuss/networking>
- World-class networking training is available from Cisco. You can view current offerings at this URL:
<http://www.cisco.com/en/US/learning/index.html>



CHAPTER 1

Installing the FlexWAN and Enhanced FlexWAN Modules

This chapter contains the following sections:

- [Preparing to Install the FlexWAN or Enhanced FlexWAN Module, page 1-1](#)
- [Installing the FlexWAN and Enhanced FlexWAN Modules, page 1-3](#)
- [Installing a FlexWAN or Enhanced FlexWAN Module Port Adapter, page 1-6](#)

Preparing to Install the FlexWAN or Enhanced FlexWAN Module



Note

Before you can install the FlexWAN or Enhanced FlexWAN modules, you must install at least one supervisor engine in the chassis. Throughout this publication, the term *supervisor engine* refers to Supervisor 720 Engine.

The following tools and equipment are required to install the FlexWAN and Enhanced FlexWAN modules:

- 3/16-inch flat-blade screwdriver for the captive installation screws on the FlexWAN and Enhanced FlexWAN modules.
- Antistatic mat or antistatic foam.
- Your own electrostatic discharge (ESD)-prevention equipment or the disposable grounding wrist strap included with all upgrade kits, field-replaceable units (FRUs), and spares.

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. Port adapters and processor modules consist of printed circuit boards that are fixed in metal carriers. Electromagnetic interference (EMI) shielding and connectors are integral components of the carrier. Although the metal carrier helps to protect the board from ESD, use a preventive antistatic strap during handling.

Follow these guidelines for preventing ESD damage:

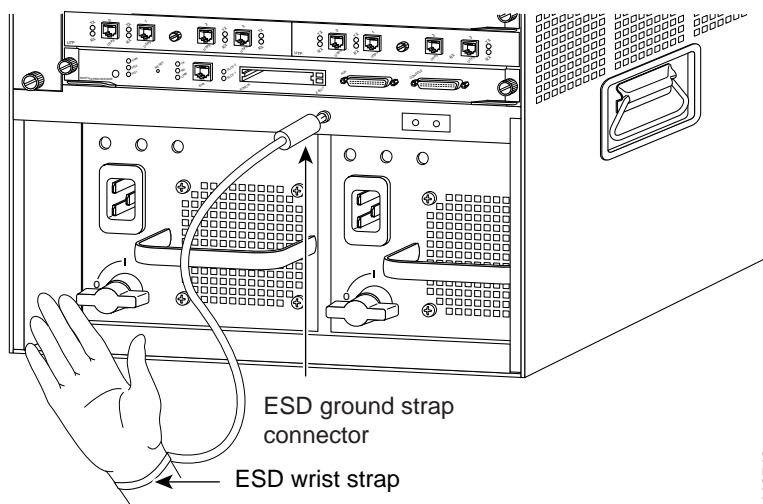
- Always use an ESD wrist or ankle strap, and ensure that it makes maximum contact with the skin. Make sure that the wrist or ankle strap is in contact with bare skin.
- Avoid contact between the printed circuit boards and clothing. The wrist strap only protects components from ESD voltages on the body; ESD voltages on clothing can still cause damage.
- The disposable ESD grounding strap supplied with field replaceable units (FRUs) has a metal clip at one end. Attach the metal clip (equipment end of the strap) to an unfinished (bare metal) chassis surface.
- The Catalyst 7600 series chassis also has a built-in ESD grounding connector. This is a banana plug connector and is identified by the ground symbol next to the connector. See [Figure 1-1](#) for an example of a chassis ESD wrist strap connection.
- When installing a component, use any available ejector levers or captive installation screws to properly seat the bus connectors in the backplane or midplane. These devices prevent accidental removal, provide proper grounding for the system, and help to ensure that bus connectors are properly seated.
- When removing a component, use any available ejector levers or captive installation screws to release the bus connectors from the backplane or midplane.
- Handle carriers by available handles or edges only; avoid touching the printed circuit boards or connectors.
- Place a removed component board-side-up on an antistatic surface or in a static shielding container. If you plan to return the component to the factory, immediately place it in a static shielding container.
- Never attempt to remove the printed circuit board from the metal carrier.



Caution

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

Figure 1-1 Example of Chassis ESD Wrist Strap Ground



Installing the FlexWAN and Enhanced FlexWAN Modules



Warning

Only trained and qualified personnel should be allowed to install or replace this equipment.

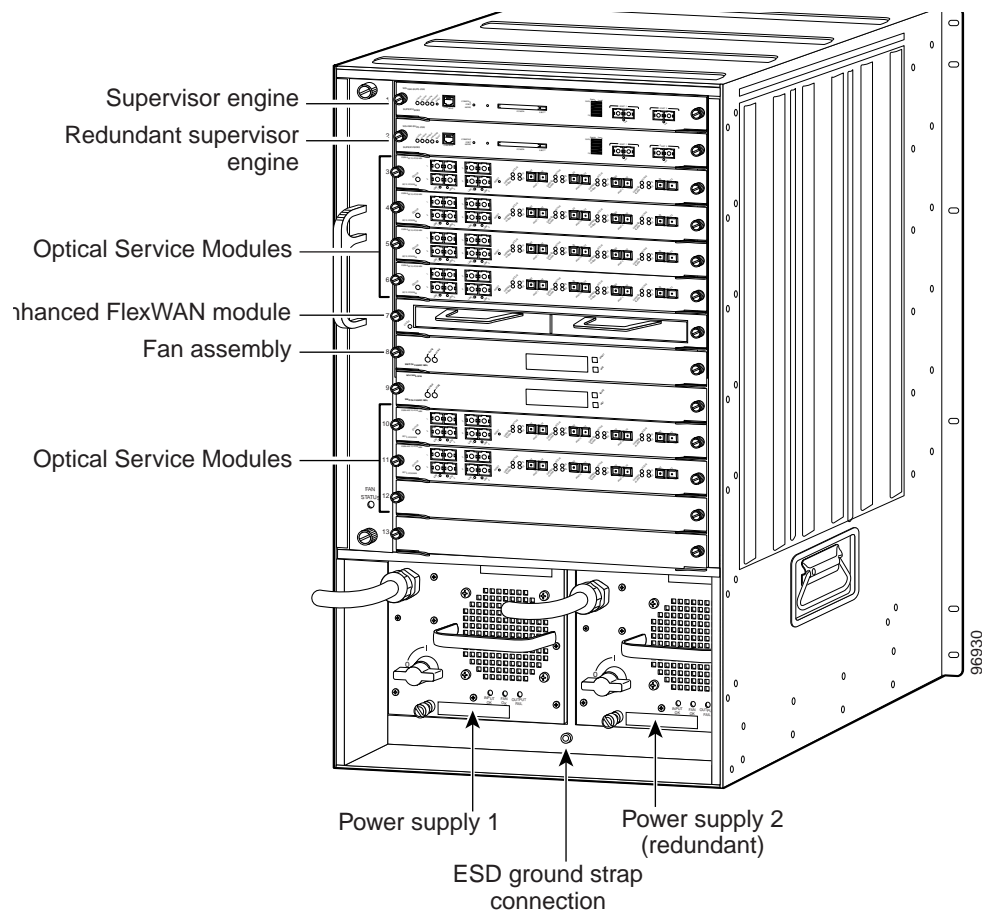
In the procedure that follows, the FlexWAN and Enhanced FlexWAN modules are installed into the horizontal slots of a Cisco 7613 router chassis. (see [Figure 1-2](#)).



Note

The FlexWAN and Enhanced FlexWAN modules are not supported without port adapters. You must install at least one port adapter before installing the module in the chassis.

Figure 1-2 Slots on the Cisco 7613 Router



To install the FlexWAN or Enhanced FlexWAN modules, follow these steps:

Step 1

Make sure that you take the necessary precautions to prevent ESD damage.

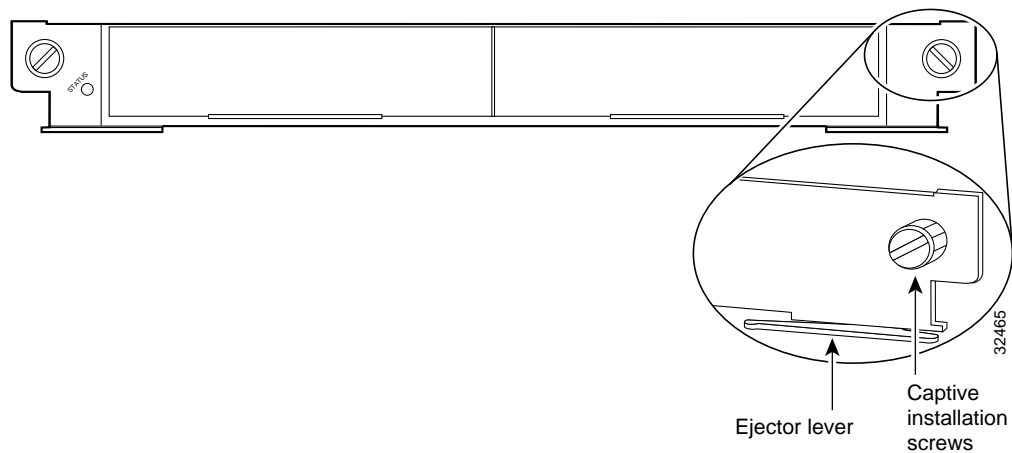


Caution

Handle modules by the carrier edges only. Always use an ESD wrist strap when handling modules or coming into contact with internal components.

- Step 2 Install port adapters on the FlexWAN or Enhanced FlexWAN module (see the “[Installing a FlexWAN or Enhanced FlexWAN Module Port Adapter](#)” section on page 1-6). Tighten any screws provided to secure the port adapter.
- Step 3 Choose a slot for the FlexWAN or Enhanced FlexWAN module.
- Step 4 Use a screwdriver to loosen the captive installation screws that secure the switching-module filler plate (or the existing switching module) from the desired slot, if present.
- Step 5 Remove the switching-module filler plate (or the existing switching module), if present.
- Step 6 Hold the module handle with one hand, and place your other hand under the carrier to support the module. Do not touch the printed circuit boards or connector pins.
- Step 7 Place the module in the slot. Align the notch on the sides of the module carrier with the groove in the slot.
- Step 8 Keep the modules at a 90-degree orientation to the backplane, and carefully slide the module into the slot until the module faceplate contacts the ejector levers (see [Figure 1-3](#)).

Figure 1-3 Ejector Levers and Captive Installation Screws



- Step 9 Use the thumb and forefinger of each hand and simultaneously push in the left and right levers to fully seat the module in the backplane connector.



Caution Always use the ejector levers when installing or removing modules. A module that is partially seated in the backplane causes the system to halt and subsequently crash.

- Step 10 Tighten the captive installation screws on the left and right ends of the module.
- Step 11 Enter the **show module** command to verify that the system acknowledges the new module and has brought it online.

The following example shows the output of the **show module** command:

```

Router# show module

Mod Ports Card Type                               Model                               Serial No.
-----
  5     2 Supervisor Engine 720 (Active)         WS-SUP720-BASE                     SAD0719027M
  6     0 2 port adapter Enhanced FlexWAN        WS-X6582-2PA                       SAD073103PD

Mod MAC addresses                               Hw   Fw       Sw           Status
-----
  5  000c.ce63.e290 to 000c.ce63.e293          2.1  7.7(1)    12.2(TETONS_ Ok
  6  00e0.aabb.cc00 to 00e0.aabb.cc3f          1.x  12.2(TETONS_ 12.2(TETONS_ Ok

Mod Sub-Module                               Model                               Serial                               Hw   Status
-----
  5 Policy Feature Card 3                     WS-F6K-PFC3A                       SAD072000G6                       1.1  Ok
  5 MSFC3 Daughterboard                      WS-SUP720                           SAD072001YS                       1.2  Ok

Mod Online Diag Status
-----
  5 Pass
  6 Pass
-----

```

**Note**

The *status* field in the output of the **show module** command indicates by “Ok” that the module is operational.

The **show module** command displays “Ok” status and “Mod Online Diag Status” only after the FlexWAN or Enhanced FlexWAN module has booted completely. While the FlexWAN or Enhanced FlexWAN module is booting (the STATUS LED is orange or red), the “Ok” status and the “Mod Online Diag Status” is unknown.

Step 12 After you install the FlexWAN or Enhanced FlexWAN modules, you must connect the port adapter cables and configure the port adapter interfaces.

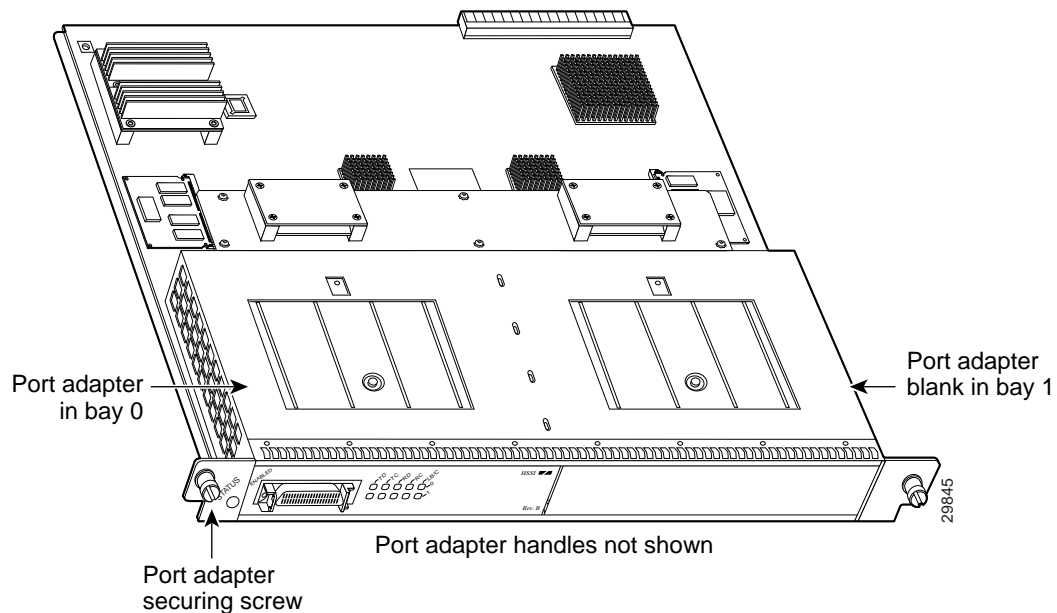
For complete cabling and configuration information for the port adapters, refer to the documentation that shipped with your port adapter.

Installing a FlexWAN or Enhanced FlexWAN Module Port Adapter

This section describes how to install a port adapter in the FlexWAN or Enhanced FlexWAN module in the Catalyst 6500 series switches or Cisco 7600 series routers.

You can install port adapters in either port adapter bay 0 or port adapter bay 1. [Figure 1-4](#) shows one PA-H port adapter installed in port adapter bay 0 on a FlexWAN or Enhanced FlexWAN module.

Figure 1-4 Port Adapter Installed in Bay 0



Required Tools and Equipment

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

- Any specific cables for your port adapter
- Number 2 Phillips screwdriver
- Your own electrostatic discharge (ESD)-prevention equipment or the disposable grounding wrist strap included with all upgrade kits, field-replaceable units (FRUs), and spares
- Antistatic mat
- Antistatic container

Handling Port Adapters

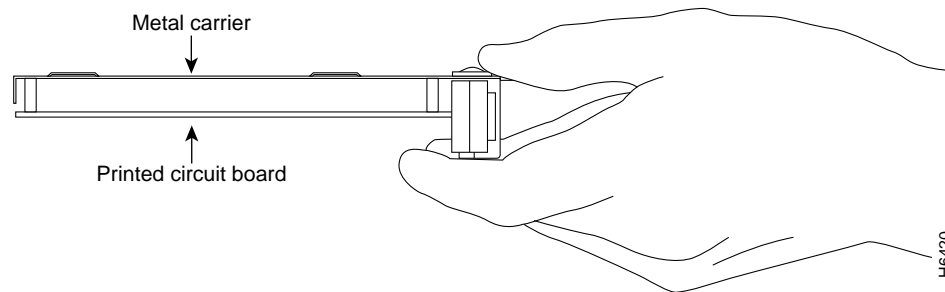
Each port adapter circuit board is mounted to a metal carrier and is sensitive to electrostatic discharge (ESD) damage.



Caution

Always handle the port adapter by the carrier edges and handle. Never touch the port adapter's components or connector pins.

Figure 1-5 Handling a Port Adapter



Caution

To prevent system problems, do not remove port adapters from the FlexWAN or Enhanced FlexWAN modules or attempt to install other port adapters on the modules when the module is operating.

Replacing Port Adapters

Although the FlexWAN or Enhanced FlexWAN module supports online insertion and removal, individual port adapters do not. To replace port adapters, you must first remove the module from the chassis, and then install or replace the port adapters as required.

When a Port Adapter Is Not in Use

When a port adapter slot is not in use, a blank port adapter must fill the empty slot to allow the router or switch to conform to electromagnetic interference (EMI) emissions requirements and to allow proper airflow across the port adapters.

If there is a blank port adapter on the FlexWAN or Enhanced FlexWAN module in which you want to install a new port adapter, you must first remove the module from the chassis, and then remove the blank port adapter.

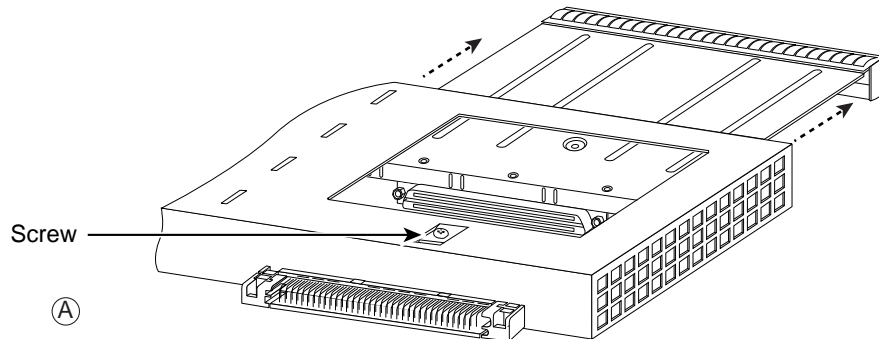
Installing a New Port Adapter in an Enhanced FlexWAN Module

This section describes how to first remove a port adapter from an Enhanced FlexWAN module, then how to install a new port adapter into its bay. (The procedure for the FlexWAN module is similar.)

Note: You must first remove the Enhanced FlexWAN Module from the chassis before removing a port adapter from the Enhanced FlexWAN Module.

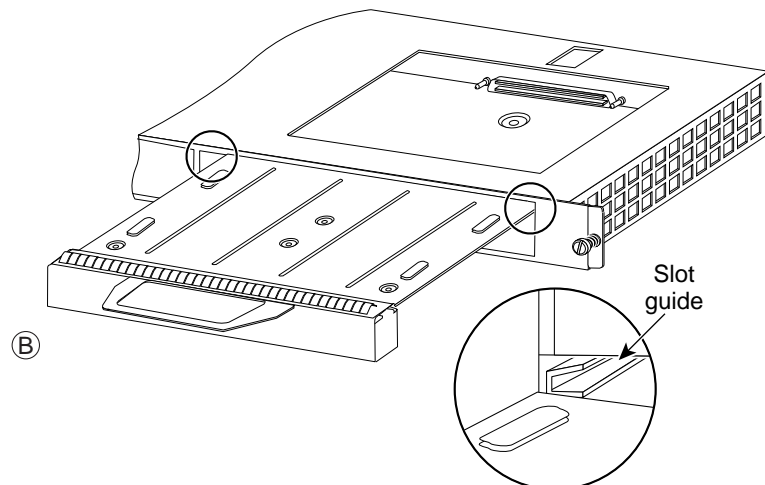
Step 1

To remove the port adapter, remove the screw that secures the port adapter (or blank port adapter). (See A.)



Step 2

With the screw removed, grasp the handle on the front of the port adapter (or blank port adapter) and carefully pull it out of its bay, away from the edge connector at the rear of the bay. (See A.)



Step 3

To install the port adapter, carefully align the port adapter carrier between the upper and the lower edges of the port adapter bay. (See B.)

Step 4

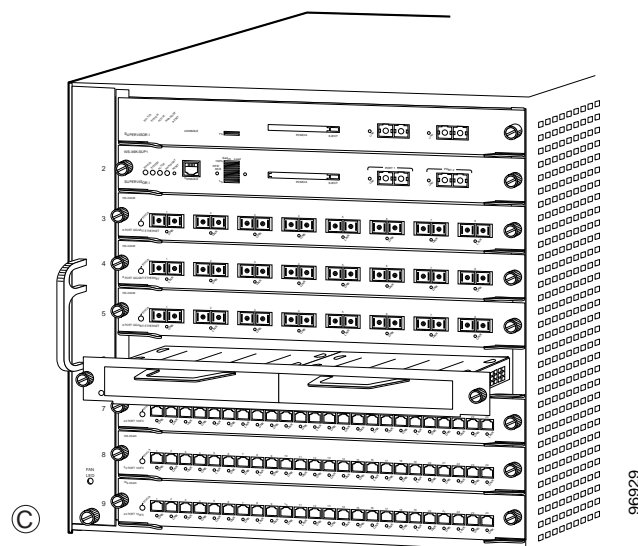
Carefully slide the new port adapter into the port adapter bay until the connector on the port adapter is completely seated in the connector at the rear of the port adapter slot. (See B.)

Step 5

Install the screw in the rear of the port adapter bay. Do not overtighten the screw. (See A.)

Step 6

Reinstall the Enhanced FlexWAN Module in the chassis, and tighten the captive installation screw on each side of the Enhanced FlexWAN Module faceplate. (See C.)



Warnings and Cautions

Observe the following warnings and cautions when installing or removing port adapters.



Do not slide a port adapter all the way into the slot until you have connected all the required cables.



To prevent jamming the carrier between the upper and the lower edges of the port adapter slot, and to ensure that the edge connector at the rear of the port adapter mates with the connection at the rear of the port adapter slot, make certain that the carrier is positioned correctly.



During this procedure, wear grounding wrist straps to avoid ESD damage to the card. Do not directly touch the backplane with your hand or any metal tool, or you could shock yourself.



Blank faceplates and cover panels serve three important functions: they prevent exposure to hazardous voltages and currents inside the chassis; they contain electromagnetic interference (EMI) that might disrupt other equipment; and they direct the flow of cooling air through the chassis. Do not operate the system unless all cards, faceplates, front covers, and rear covers are in place.



This equipment must be installed and maintained by service personnel as defined by AS/NZS 3260. Incorrectly connecting this equipment to a general-purpose outlet could be hazardous. The telecommunications lines must be disconnected 1) before unplugging the main power connector or 2) while the housing is open, or both.



CHAPTER 2

Replacing or Upgrading Module Memory

This chapter contains the following sections:

- [Notes and Cautions, page 2-1](#)
- [Removing SODIMMs, page 2-2](#)
- [Installing New SODIMMs, page 2-4](#)
- [Checking an SDRAM Upgrade or Replacement, page 2-5](#)

This chapter describes the procedure for removing and replacing the memory on the FlexWAN module in the Catalyst 6500 series switches or Cisco 7600 series routers.

The *synchronous dynamic random-access memory* (SDRAM) on the Catalyst FlexWAN module is contained in two *small outline dual inline memory modules* (SODIMMs) (see [Figure 2-1 on page 2-2](#)). Depending on your system configuration, you might need to upgrade SDRAM. Also, if a system problem is determined to be caused by a SODIMM, you may need to replace the SODIMM.

Notes and Cautions



Note

The FlexWAN module has 64 MB of ECC SDRAM (MEM-C6K-WAN-64M) per port adapter bay (128 MB for the entire FlexWAN module). It can be upgraded to 128 MB ECC SDRAM (MEM-C6K-WAN-128M) for each port adapter bay (256 MB for the entire FlexWAN module). ECC (error correction code) SDRAM is memory that is able to detect and correct some SDRAM errors without user intervention.



Note

The default ECC SDRAM memory options for each of the two port adapter bays in the Enhanced FlexWAN module is 256 MB (MEM-CC-WAN-256M) per bay. You can upgrade to 512 MB (MEM-CC-WAN-512M) per bay.



Note

You should use only 100-MHz SDRAM SODIMMs. A Cisco part number is inscribed on each SODIMM.

**Caution**

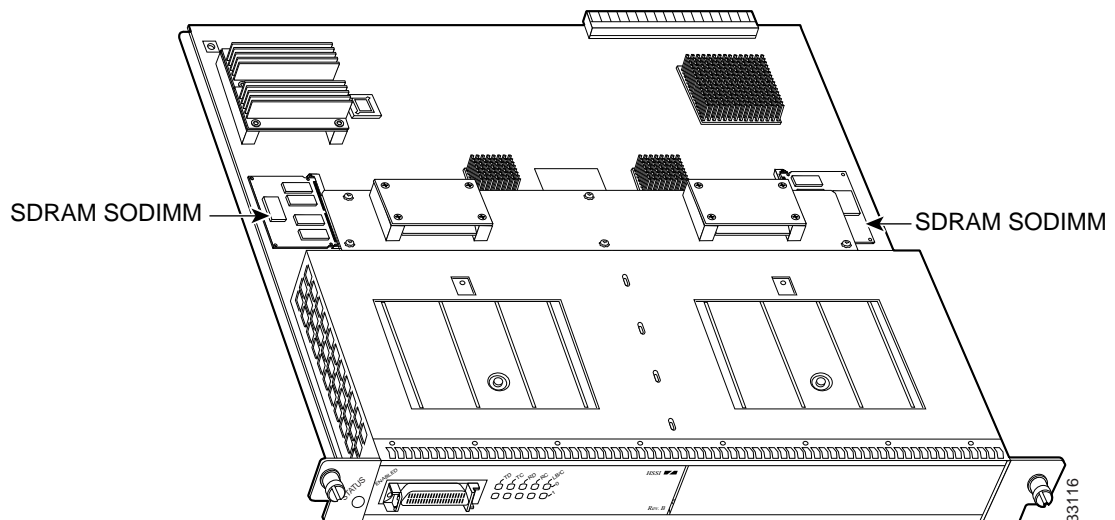
To prevent damage through electrostatic discharge (ESD), handle the SODIMMs by the card edges only (see [Figure 2-3 on page 2-4](#)). Place the removed SODIMMs on an antistatic mat and store them in an antistatic container.

Removing SODIMMs

To remove the existing SODIMMs, follow these steps:

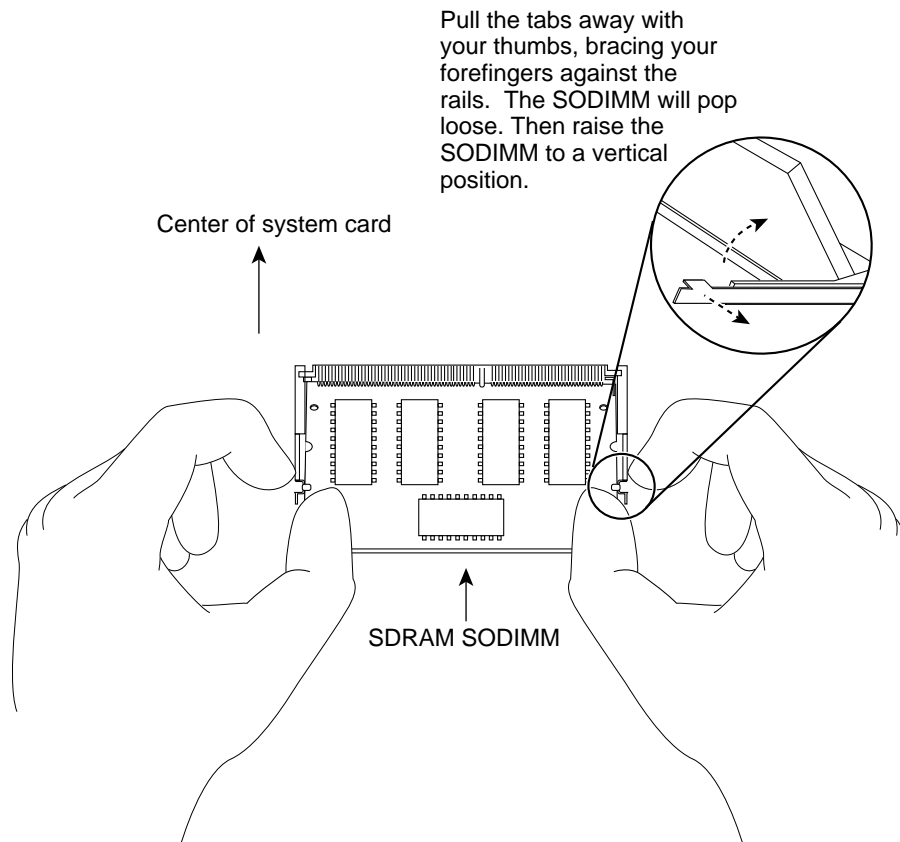
- Step 1** Remove the FlexWAN or Enhanced FlexWAN module from the system.
- Step 2** Place the FlexWAN or Enhanced FlexWAN module on an antistatic mat or pad and ensure that you are wearing an antistatic device, such as a wrist strap.
- Step 3** Locate the SODIMMs, as shown in [Figure 2-1](#).

Figure 2-1 Location of the SDRAM SODIMMs



- Step 4** Release the spring clips from the SODIMM that you want to remove, then release the SODIMM from the socket (see [Figure 2-2](#)).

Figure 2-2 Releasing the SODIMM Spring Clips



- Step 5** When both ends of the SODIMM are released from the socket, grasp the ends of the SODIMM with your thumb and forefinger and pull the SODIMM completely out of the socket.
- Handle the edges of the SODIMM only; avoid touching the memory modules, pins, or the metal traces or *fingers* along the socket edge.
- Step 6** Place the SODIMM in an antistatic container to protect it from ESD damage.
- Step 7** To remove the remaining SODIMM, repeat Step 4 through Step 6 in this procedure.

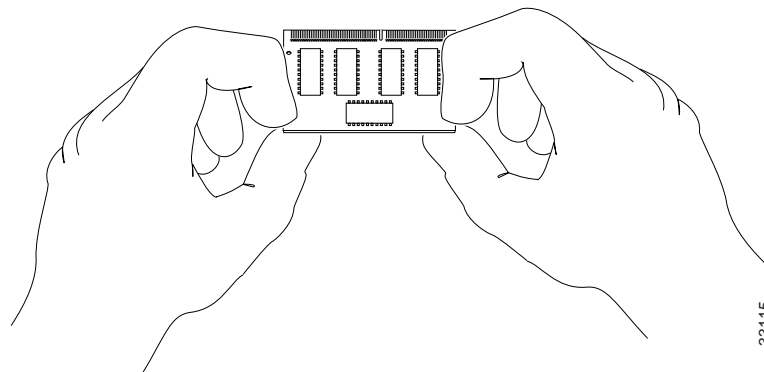
This completes the SODIMM removal procedure. Proceed to the next section for the procedure to install the new SODIMMs.

Installing New SODIMMs

This section describes how to install a SODIMM into a FlexWAN or Enhanced FlexWAN module.

SODIMMs are sensitive components that are susceptible to ESD damage. Handle SODIMMs by the edges only as shown in [Figure 2-3](#)—avoid touching the memory modules, pins, or *traces* (that is, the metal fingers along the connector edge of the SODIMM).

Figure 2-3 Handling a SODIMM



To install the new SODIMMs, follow these steps:

-
- Step 1** Remove a new SODIMM from the antistatic container.
 - Step 2** Hold the SODIMM component-side-up, with the connector edge (the metal fingers) away from you.
 - Step 3** Hold the sides of the SODIMM between your thumb and middle finger, with your forefinger against the far edge, opposite the connector edge.
 - Step 4** Tilt the SODIMM to approximately the same angle as the socket, and insert the connector edge into the socket.

When inserting SODIMMs, use firm but not excessive pressure.



Tip If you damage a socket, you have to return the FlexWAN or Enhanced FlexWAN module to the factory for repair.

- Step 5** To install the remaining SODIMM, repeat Step 1 through Step 5.
- Step 6** When both SODIMMs are installed, check all four alignment holes (two on each SODIMM) and ensure that the spring clip is visible. If the spring retainer is not visible, the SODIMM is not seated properly.
- Step 7** If a SODIMM appears misaligned, carefully remove it and reseat it in the socket. Push the SODIMM firmly back into the socket until the retainer springs snap into place.
- Step 8** Reinstall the FlexWAN or Enhanced FlexWAN module in the chassis and restart the system for an installation check (for details, see the next section, "[Checking an SDRAM Upgrade or Replacement](#)").

This completes the SDRAM SODIMM replacement procedure.

Checking an SDRAM Upgrade or Replacement

If, after a SDRAM upgrade or replacement, the system fails to boot properly, or if the console terminal displays a checksum or memory error, check the following:

1. Ensure that all SODIMMs are installed correctly.
2. If necessary, shut down the system and remove the FlexWAN or Enhanced FlexWAN module.
3. Check the SODIMMs by looking straight down on them and then at eye level. When properly installed, the SODIMMs should be aligned at the same angle and the same height.
4. If a SODIMM appears to stick out or rest in the socket at a different angle from the others, remove it and reinsert it.
5. Then replace the FlexWAN or Enhanced FlexWAN module and reboot the system for another installation check.

**Note**

The SDRAM SODIMM sockets must contain SODIMMs of the same size and speed or the system cannot operate. SODIMMs must be 100 MHz or faster.

6. If after several attempts the system fails to restart properly, contact a service representative for assistance.
7. Before you call, note any error messages, unusual LED states, or other indications that might help solve the problem.



CLI Commands for the FlexWAN and Enhanced FlexWAN Modules

Table 3-1 lists the CLI commands for displaying FlexWAN or Enhanced FlexWAN module status, configuration, and statistical information, as well as the commands for debugging purposes. Enter these commands from the Multilayer Switch Feature Card (MSFC) console.

**Note**

For more information on these commands, see:

<http://www.cisco.com/univercd/cc/td/doc/product/core/cis7600/software/122sx/cmdref/index.htm>

Table 3-1 CLI Commands for the FlexWAN and Enhanced FlexWAN Modules

Command	Options	Description
Router# <code>show cwan</code>	stats vlans	Displays WAN port statistics. Displays hidden VLAN-to-WAN interface mapping.
Router# <code>dir cwan</code>	cwan[mod_num]/bay-bootflash: cwan[mod_num]/bay-disk0	Displays the FlexWAN module bootflash devices. Displays the Enhanced FlexWAN module bootflash devices.
Router# <code>show fabric</code>	switching-mode utilization	Displays the module switching mode. Displays the percentage of utilization for each fabric channel.
Router# <code>show diagnostic</code>	bootup level content events schedule	Displays the coverage level for the boot-up diagnostics. Displays test information for each test and for all modules. Displays the event log for the diagnostic events. Displays the current scheduled diagnostic tasks.

REVIEW DRAFT—CISCO CONFIDENTIAL