Hardware Installation Guide for Cisco 8300 Series Secure Routers

First Published: 2025-07-31

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

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

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: This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to part 15 of the FCC rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If the equipment causes interference to radio or television reception, which can be determined by turning the equipment off and on, users are encouraged to try to correct the interference by using one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

Modifications to this product not authorized by Cisco 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.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

All printed copies and duplicate soft copies of this document are considered uncontrolled. See the current online version for the latest version.

Cisco has more than 200 offices worldwide. Addresses and phone numbers are listed on the Cisco website at www.cisco.com/go/offices.

CONTENTS

CHAPTER 1

CHAPTER 2

CHAPTER 1

Cisco 8300 Series Secure Routers

Cisco 8300 Series Secure Routers deliver secure networking simplified. Powered by the all-new secure networking processor and the unified Cisco secure networking platform, the Cisco 8300 Series Secure Routers deliver robust, platform-level security, advanced performance engineering thorough routing and SD-WAN, and on-premises, infrastructure-as-code, or cloud management flexibility that enables businesses to seamlessly scale and grow. Each class of secure routers is designed to deliver risk reduction, enhanced reliability, and future readiness.

Cisco 8300 Series Secure Routers are engineered for large branch locations and provide scalable, high-throughput connectivity with embedded platform-level security. With hardware-native assurance, post-quantum cryptography, and unified infrastructure as code, the Cisco 8300 Series enables large branches to support bandwidth-intensive applications and evolving threat landscapes with confidence.

For more information on the features and specifications, see the Cisco 8300 Series Secure Routers datasheet.

Note Sections in this documentation apply to all models of Cisco 8300 Series Secure Routers unless a reference to a specific model is made explicitly.

Chassis views

This section contains views of the power supply and I/O sides of the Cisco 8300 Series Secure Routers, showing the locations of power and signal interfaces, module slots, status indicators, and chassis identification labels:

Cisco 8300 Series Secure Routers are available in these models:

- C8375-E-G2

Figure 1: C8375-E-G2 chassis - I/O Side

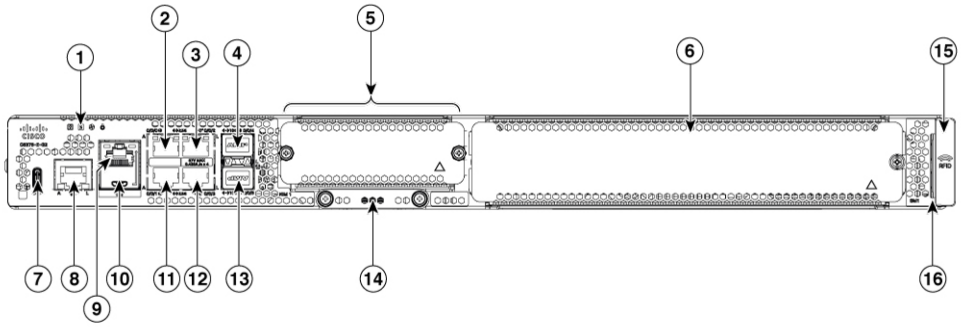


Table 1: I/O side

1	LED	2	RJ-45 mGigabitEthernet port (2.5G 0/0/0)
3	RJ-45 mGigabitEthernet port (2.5G 0/0/2)	4	SFP+/10 Gigabit Ethernet port (10G 0/0/4)
5	NIM Slot1	6	SM Slot1
7	USB Type C (3.0) (USB 0)	8	RJ-45 Gigabit Ethernet management port (1G)
9	RJ-45 Console	10	Micro-USBConsole
11	RJ-45 mGigabitEthernet port (2.5G0/0/1)	12	RJ-45 mGigabitEthernet port (2.5G0/0/3)
13	SFP+/10 Gigabit Ethernet port (10G 0/0/5)	14	M.2USB/NVMe storage
15	RFID	16	Device Label Tray

Figure 2: C8375-E-G2 chassis - PSU/Fan tray side

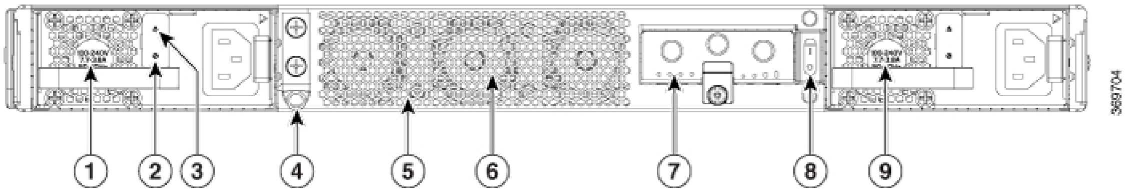


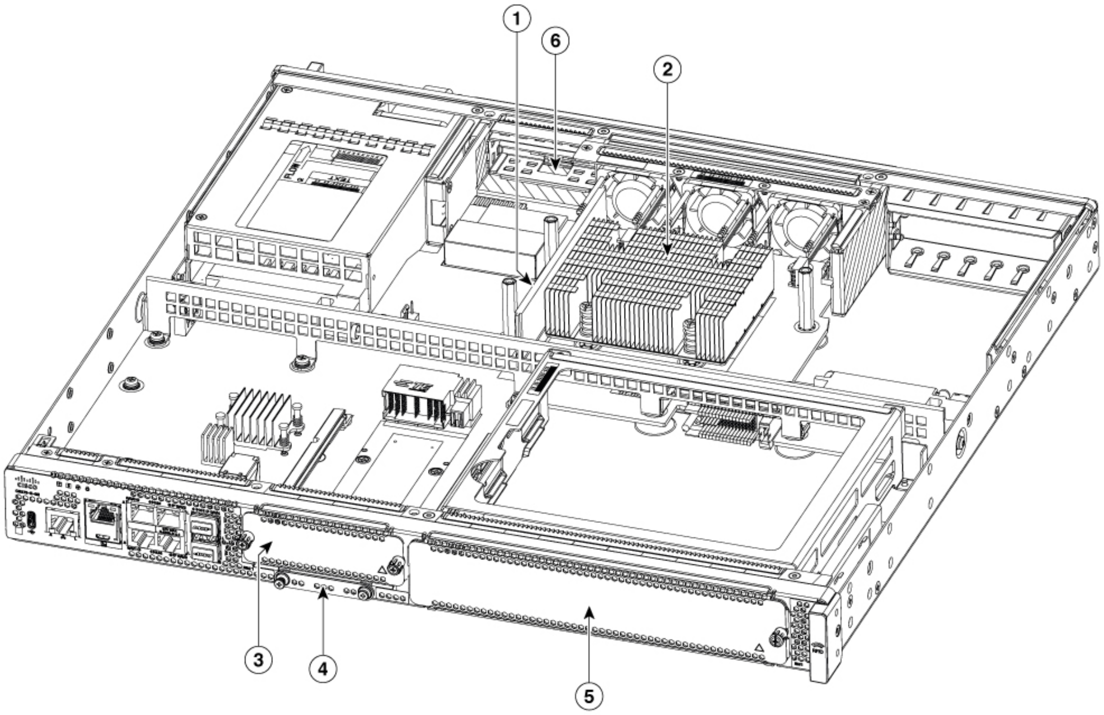
Table 2: PSU/Fan tray side

1	AC/DC power supply unit (PSU1)	2	Power, Preset, OK, LED
3	ALARM Fail LED	4	Ground lug
5	Fan tray vent	6	3-Internal Fan tray
7	PIM Slot 1	8	Power switch
9	AC/DC Power Supply Unit (PSU0)		

Platform summary

The figure shows the internal view of Cisco 8300 Series Secure Routers with components and module locations.

Figure 3: Platform summary of C8375-E-G2



1	DIMM	2	CPU
3	NIM slot	4	M.2 card slot
5	SM slot	6	PIM slot

Locating labels on Cisco 8300 Series Secure Routers

Use the Cisco Product Identification (CPI) tool to find labels on the platform. The tool provides detailed illustrations and descriptions of where labels are located on Cisco products. It includes these features:

- A search option that allows browsing for models by using a tree-structured product hierarchy
- A search field on the final results page that makes it easier to look up multiple products
- End-of-sale products clearly identified in results lists

The tool streamlines the process of locating serial number labels and identifying products. Serial number information expedites the entitlement process and is required for access to support services.

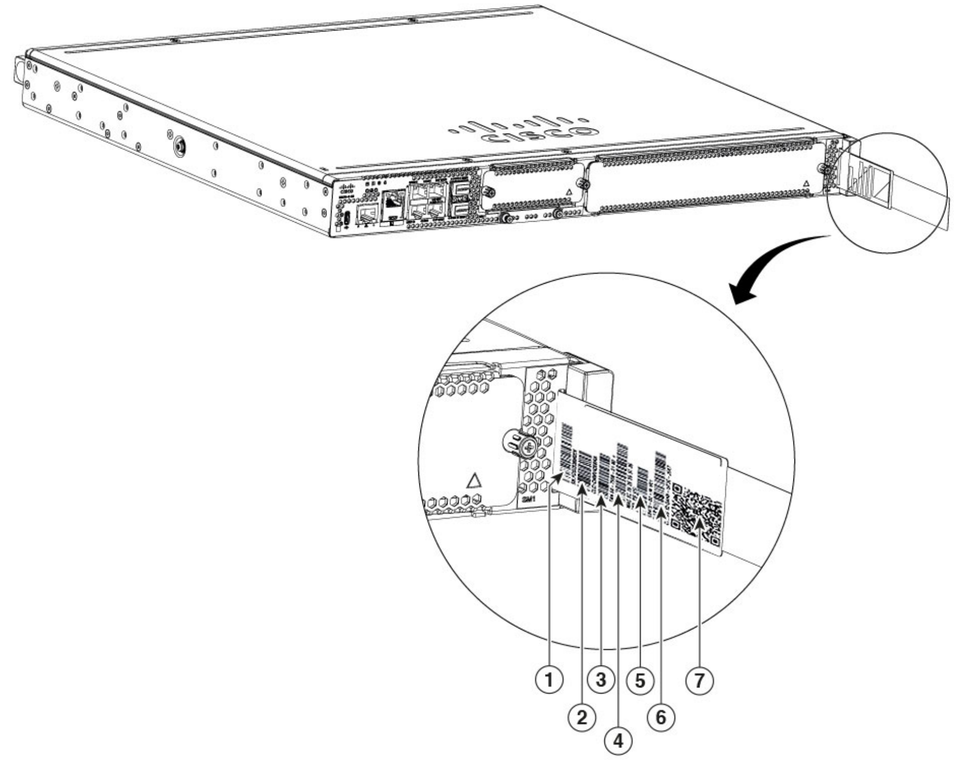
Labels on Cisco 8300 Series Secure Routers

The figure shows the location of the labels on the Cisco 8300 Series Secure Routers. Labels are located at the same location on all the Cisco 8300 Series Secure Routers.

The Serial number (SN), Common language equipment identifier (CLEI), Top Assembly Number (TAN), Product ID (PID), PID version ID (VID), and Quick response (QR) code are printed on a label on the back of the platform or on a label tray located on the chassis.

Note The RFID tags on the devices are pre-fitted and does not come with spare RFID tags.

Figure 4: Label location on a C8375-E-G2



1	SN	2	CLEI
3	TAN	4	MAC
5	PIDVID	6	Cloud ID
7	QR Code	x	

Locate product identification details

Software license

The serial number (SN), product ID (PID), version ID (VID), Cloud ID and Common Language Equipment Identifier (CLEI) are printed on a label on the bottom of the device or on the label tray.

To obtain a software license, you need the unique device identifier (UDI) of the device where the license is to be installed.

The UDI has two main components:

- Product ID (PID)
- Serial number (SN)

The UDI can be viewed using the **show license udi** command in privileged Exec mode in Cisco Internet Operating System (IOS) software.

For additional information on the UDI, see the Product Identification Standrad document on cisco.com.

Hardware features of Cisco 8300 Series Secure Routers

This section describes the hardware features of Cisco 8300 Series Secure Routers.

Built-in interface ports

The Cisco 8300 Series Secure Routers have multiple 10/100/1000 front panel ports and Small Form Pluggables.

Warning To comply with the Telcordia GR-1089 NEBS standard for electromagnetic compatibility and safety, connect the Management Ethernet ports only to intra-building or unexposed wiring or cable. The intra-building cable must be shielded and the shield must be grounded at both ends. The intra-building port(s) of the equipment or subassembly must not be metallically connected to interfaces that connect to the OSP or its wiring. These interfaces are designed for use as intra-building interfaces only (Type 2 or Type 4 ports as described in GR-1089-CORE) and require isolation from the exposed OSP cabling. The addition of Primary Protectors in not sufficient protection in order to connect these interfaces metallically to OSP wiring.

RJ45 mGIG ports or SFP+ ports

The GE and SFP ports available on the Cisco 8300 Series Secure Routers are:

mGIG ports

The mGIG RJ-45copper interface ports support 100BASE-TX,1000BASE-T, and 2500BASE_T.

SFP+ ports

The enhanced small-form-factor pluggable (SFP) ports support 10 Gbps SFP+ modules.

Removable and interchangeable modules and cards

Service Modules (SMs), Network Interface Modules (NIMs), Pluggable Interface Modules (PIMs) and M.2 USB/NVMe storage fit into external slots and can be removed or replaced without opening the chassis.

Internal slots

List of internal slots for C8375-E-G2:

- Memory

See the Cisco 8300 Series Secure Routers product page on cisco.com for a list of supported modules and interface cards.

Memory

Cisco 8300 Series Secure Routers contain DIMMs that store running configuration and routing tables and are used for packet buffering by the network interfaces.

Memory in C8375-E-G2:

- Boot/NVRAM—Stores the bootstrap program (ROM monitor) and the configuration register. The boot/NVRAM is not serviceable.
- Internal memory—Internal bootflash memory
- Removable M.2 card—Available in 32GBM.2 USB, 600GBM.2 NVMe SSD and 2TBM.2 NVMe SSD
- DRAM options
    - 1x 16GB DDR5 (default)
    - 1x 32GB DDR5 (upgrade)

Power supply

Cisco 8300 Series Secure Routers support a variety of power supply configurations. These devices have power supplies that are field replaceable and externally accessible. The table summarizes the power options:

Table 3: Field replaceable unit power options

Model	AC Input PSU	PSU with Integrated PoE	Dual, Hot Swap	DC Input PSU
C8375-E-G2	Y	Y	Y	Y

LEDs for Cisco 8300 Series Secure Routers

Table 4: LED indicators for C8375-E-G2

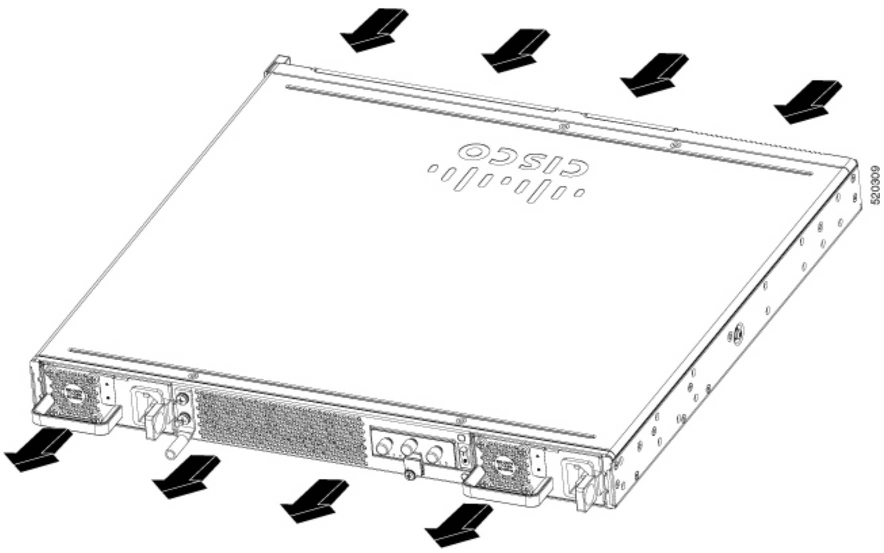
LED	Color	Description
PWR	Green/Amber	**Power Supply Status** Off: The system is powered off Amber: A Power Supply in the system is not functioning correctly Green: All installed PSUs are operating correctly
STATUS	Green/Amber/Red	**System Status** Blinking Amber: The system is booting Blinking Red: The system has failed a hardware integrity error Amber: Rommon has completed booting and system is at Rommon prompt or booting platform software Green: Normal System Operation
ENV	Green/Amber/Red	**Environmental Status** Off: Monitor is not active Red: The system has detected a critical overcurrent event and may shut down Blinking Amber: One or more temperature sensors in the system are outside the acceptable range Amber: One or more fans in the system are outside the acceptable range Green: All temperature sensors and fans in the system are within acceptable range
BEACON	Blue	Off: System is normal Blinking Blue: Beacon purpose
USB CON	Green	**USB Console Active** Green indicates that the active console port is USB

LED	Color	Description
RJ-45 CON	Green	**Serial Console Active** Green indicates that RJ-45 is the active console port
RJ-45 Ethernet Ports A (Active)	Green	**Activity status** Off: No data Blinking Green: Tx/Rx data
RJ-45 Ethernet Ports L (Link)	Green/Amber	**Link status** Off: No data Green: Link up Amber: POE power fault and link is down **Note** The C8375-E-G2 supports 2 PoE Ports (802.3bt, 90W per port) on port 0/0/2 and 0/0/3
SFP Ports L (Link)	Green/Amber	**SFP port 0/1 Link LED** Off: No Link (or SFP not present) Green: Link established Amber: The SFP is not supported, or it is in a fault state

Chassis ventilation

The chassis temperature is regulated with internal fans. An onboard temperature sensor controls the fan speed. The fans are always on when the device is powered on. Under all conditions, the fans operate at the slowest speed possible to conserve power and reduce noise. When necessary, the fans operate at higher speeds under conditions of higher ambient temperature and altitude.

Figure 5: Airflow of C8375-E-G2

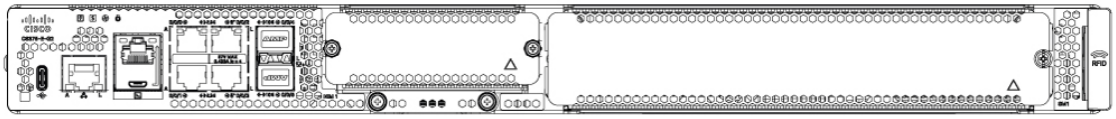


Slots, subslots-bay, ports, and interfaces

The Cisco 8300 Series Secure Routers support interface modules: Service Modules (SM) and Network Modules (NIMs) and Pluggable Interface Modules (PIMs).

The C8375-E-G2 router supports Service Modules (SM) and Network Modules (NIMs) and Pluggable Interface Modules (PIMs).

Figure 6: C8375-E-G2 interfaces



In all cases, the device designates its interfaces using a 3-tuple notation that lists the slot, bay, and port. The 3-tuple value is zero based. An example of a 3-tuple is 0/1/2. This refers to slot 0, the second bay in slot 0 (the first bay is 0 so the second bay is 1), and the third port in bay 1. See the following table for more examples.

Table 5: Slot, subslot-bay and port numbering

3-Tuple Example	Slot	Bay	Port
0/1/2	0	2nd	3rd
0/0/1	0	1st	2nd
1/1/1	1	2nd	2nd

- Slots and bays are numbered from the left to the right, and from the top to the bottom.
- The USB port is named USB0. It doesn’t haveslot or bay numbers.

Note USB0 can be used to insert flash drives.

Slot numbering

Slots are numbered 0, 1, and 2.

Slot 0

These are the main features about Slot 0:

- Slot 0 is reserved for integrated ports and NIMs, it can be used for either SM or NIM.
- NIMs are designated by the number of the first slot that they occupy. A double-wide SM occupies two slots, but its designation is only the left-most slot number.
- The ten GE ports (or native interface ports) always reside in slot 0 and bay 0. The ports are called Gigabitethernet 0/0/0, Gigabitethernet 0/0/1, Gigabitethernet 0/0/2, and Gigabitethernet 0/0/3 (up to as many ports supported on the particular router).

Subslot and bay numbering

- Integrated devices, also known as integrated ports or FPGEs, and NIMs reside in a fixed section of bay 0.
- Motherboard NIMs bays start at bay 1 because the integrated devices and integrated NIMs take up bay 0.

CHAPTER 2

Prepare for installation

This chapter provides preinstallation information, such as recommendations and requirements that must be met before installing your platform. Before you begin, inspect all items for shipping damage. If anything appears to be damaged or if you encounter problems installing or configuring your platform, contact customer service.

Standard warning statements

This section describes the warning definition and then lists core safety warnings grouped by topic.

Warning **Statement 1071**—Warning Definition

IMPORTANT SAFETY INSTRUCTIONS

Before you work on any equipment, be aware of the hazards involved with electrical circuitry and be familiar with standard practices for preventing accidents. Read the installation instructions before using, installing, or connecting the system to the power source. Use the statement number at the beginning of each warning statement to locate its translation in the translated safety warnings for this device.

SAVE THESE INSTRUCTIONS

General safety warnings

Take note of these general safety warnings:

Note

Statement 407—Japanese Safety Instruction

You are strongly advised to read the safety instruction before using the product.

https://www.cisco.com/web/JP/techdoc/pldoc/pldoc.html

When installing the product, use the provided or designated connection cables/power cables/AC adapters.

〈製品使用における安全上の注意〉

www.cisco.com/web/JP/techdoc/index.html

接続ケーブル、電源コードセット、**AC**アダプタ、バッテリなどの部品は、必ず添付品または指定品をご使用ください。添付品・指定品以外をご使用になると故障や動作不良、火災の原因となります。また、電源コードセットは弊社が指定する製品以外の電気機器には使用できないためご注意ください。

Warning

Statement 445—Connect the Chassis to Earth Ground

To reduce the risk of electric shock, connect the chassis of this equipment to permanent earth ground during normal use.

Note

Statement 1005—Circuit Breaker

This product relies on the building's installation for short-circuit (overcurrent) protection. To reduce risk of electric shock or fire, ensure that the protective device is rated not greater than: 20A.

Warning

Statement 1008—Class 1 Laser Product

This product is a Class 1 laser product.

Warning

Statement 1017—Restricted Area

This unit is intended for installation in restricted access areas. Only skilled, instructed, or qualified personnel can access a restricted access area.

Warning

Statement 1022—Disconnect Device

To reduce the risk of electric shock and fire, a readily accessible disconnect device must be incorporated in the fixed wiring.

Warning

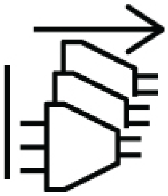
Statement 1024—Ground Conductor

This equipment must be grounded. To reduce the risk of electric shock, never defeat the ground conductor or operate the equipment in the absence of a suitably installed ground conductor. Contact the appropriate electrical inspection authority or an electrician if you are uncertain that suitable grounding is available.

Warning

Statement 1028—More Than One Power Supply

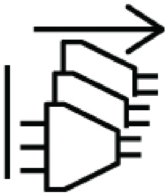
This unit might have more than one power supply connection. To reduce risk of electric shock, remove all connections to de-energize the unit.



Warning

Statement 1028—More Than One Power Supply

This unit might have more than one power supply connection. To reduce risk of electric shock, remove all connections to de-energize the unit.



Warning

Statement 1029—Blank Faceplates and Cover Panels

Blank faceplates and cover panels serve three important functions: they reduce the risk of electric shock and fire, 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.

Warning **Statement 1032**—Lifting the Chassis

To prevent personal injury or damage to the chassis, never attempt to lift or tilt the chassis using the handles on modules, such as power supplies, fans, or cards. These types of handles are not designed to support the weight of the unit.

Warning **Statement 1035**—Proximity to Water

Do not use this product near water, for example, near a bathtub, wash bowl, kitchen sink, laundry tub, in a wet basement, or near a swimming pool.

Warning **Statement 1038**—Telephone Use During an Electrical Storm

Avoid using a telephone (other than a cordless type) during an electrical storm. There may be a risk of electric shock from lightning.

Warning **Statement 1039**—Telephone Use by Gas Leak

To reduce the risk of ignition, do not use a telephone in the vicinity of a gas leak.

Warning **Statement 1041**—Disconnect Telephone Network Cables

Before opening the unit, disconnect the telephone network cables to avoid contact with telephone network voltages.

Warning **Statement 1055**—Class 1/1M Laser

Invisible laser radiation is present. Do not expose to users of telescopic optics. This applies to Class 1/1M laser products.

Warning **Statement 1056**—Unterminated Fiber Cable

Invisible laser radiation may be emitted from the end of the unterminated fiber cable or connector. Do not view directly with optical instruments. Viewing the laser output with certain optical instruments, for example, eye loupes, magnifiers, and microscopes, within a distance of 100 mm, may pose an eye hazard.

Warning **Statement 1073**—No User-Serviceable Parts

There are no serviceable parts inside. To avoid risk of electric shock, do not open.

Warning **Statement 1074**—Comply with Local and National Electrical Codes

To reduce risk of electric shock or fire, installation of the equipment must comply with local and national electrical codes.

Warning **Statement 1086**—Replace Cover on Power Terminals

Hazardous voltage or energy may be present on power terminals. To reduce the risk of electric shock, make sure the power terminal cover is in place when the power terminal is not being serviced. Be sure uninsulated conductors are not accessible when the cover is in place.

Warning **Statement 1089**—Instructed and Skilled Person Definitions

An instructed person is someone who has been instructed and trained by a skilled person and takes the necessary precautions when working with equipment.

A skilled person or qualified personnel is someone who has training or experience in the equipment technology and understands potential hazards when working with equipment.

There are no serviceable parts inside. To avoid risk of electric shock, do not open.

Warning **Statement 1090**—Installation by Skilled Person

Only a skilled person should be allowed to install, replace, or service this equipment. See statement 1089 for the definition of a skilled person.

There are no serviceable parts inside. To avoid risk of electric shock, do not open.

Warning **Statement 1091**—Installation by an Instructed Person

Only an instructed person or skilled person should be allowed to install, replace, or service this equipment. See statement 1089 for the definition of an instructed or skilled person.

There are no serviceable parts inside. To avoid risk of electric shock, do not open.

Warning **Statement 1100—**Before Making Telecommunication Network Connection

High touch/leakage current—Permanently connected protective earth ground is essential before connecting to the telecommunication network.

Network Equipment-Building System (NEBS) statements

NEBS describes the environment of a typical United States Regional Bell Operating Company (RBOC) central office. NEBS is the most common set of safety, spatial, and environmental design standards applied to telecommunications equipment in the United States. It is not a legal or regulatory requirement, but rather an industry requirement.

The following NEBS statements apply to the :

Warning **Statement 7003**—Shielded Cable Shielded Cable Requirements for Intrabuilding Lightning Surge

The intrabuilding port(s) of the equipment or subassembly must use shielded intrabuilding cabling/wiring that is grounded at both ends.

The following port(s) are considered intrabuilding ports on this equipment:

RJ-45 Copper Ethernet Ports

Note **Statement 7004—**Special Accessories Required to Comply with GR-1089 Emission and Immunity Requirements

To comply with the emission and immunity requirements of GR-1089, shielded cables are required for the following ports:

RJ-45 Copper Ethernet Ports

Warning **Statement 7005**—Intrabuilding Lightning Surge and AC Power Fault

The intrabuilding port(s) of the equipment or subassembly must not be metallically connected to interfaces that connect to the outside plant (OSP) or its wiring. These interfaces are designed for use as intrabuilding interfaces only (Type 2 or Type 4 ports as described in GR-1089-CORE) and require isolation from the exposed OSP cabling. The addition of primary protectors is not sufficient protection to connect these interfaces metallically to OSP wiring.

This statement applies to the intrabuilding ports listed below:

RJ-45 Copper Ethernet Ports

Note **Statement 7013—**Equipment Grounding Systems—Common Bonding Network (CBN)

This equipment is suitable for installations using the CBN.

Note **Statement 7016**—Battery Return Conductor

Treat the battery return conductor of this equipment as Isolated DC return (DC-I).

Note **Statement 7018—**System Recover Time

The equipment is designed to boot up in less than 30 minutes provided the neighboring devices are fully operational.

Note **Statement 8015—**Installation Location Network Telecommunications Facilities

This equipment is suitable for installation in network telecommunications facilities.

Note **Statement 8016—**Installation Location Where the National Electric Code (NEC) Applies

This equipment is suitable for installation in locations where the NEC applies.

Safety recommendations

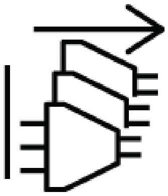
Follow these guidelines to ensure general safety:

- Never attempt to lift an object that might be too heavy for you to lift by yourself.
- Keep the chassis area clear and dust-free during and after installation.
- If you remove the chassis cover, place it in a safe place.
- Keep tools and chassis components away from walk areas.
- Do not wear loose clothing that may get caught in the chassis. Fasten any tie or scarf and roll up sleeves.
- Wear safety glasses when working under conditions that might be hazardous to your eyes.
- Do not perform any action that may create a hazard to people or makes equipment unsafe.

Safety with electricity

Warning **Statement 1028—**More Than One Power Supply

This unit might have more than one power supply connection. To reduce risk of electric shock, remove all connections to de-energize the unit.



Follow these guidelines when working on equipment powered by electricity:

- Locate the emergency power-off switch in the room in which you are working. If an electrical accident occurs, you can quickly turn off the power.
- Disconnect all power before doing the following:
  - Installing or removing a chassis
  - Working near power supplies
- Look carefully for possible hazards in your work area, such as moist floors, ungrounded power extension cables, frayed power cords, and missing safety grounds.
- Do not work alone if hazardous conditions exist
- Never assume that power is disconnected from a circuit. Always check
- Never open the enclosure of the internal power supply
- If an electrical accident occurs to another person, proceed as follows:
  - Use caution; do not become a victim yourself
  - Turn off power to the device
  - 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, use the following guidelines when working with any equipment that is disconnected from a power source but has telephone wiring or other network cabling connections:

- Never install telephone wiring during a lightning storm.
- Never install telephone jacks in wet locations unless the jack is specifically designed for it.
- Never touch uninsulated telephone wires or terminals unless the telephone line is disconnected at the network interface.

- Use caution when installing or modifying telephone lines.
- Remove power cables from all installed power supplies before opening the chassis.

Prevent electrostatic discharge damage

Electrostatic discharge (ESD) can damage equipment and impair electrical circuitry. It can occur if electronic printed circuit cards are improperly handled and can cause complete or intermittent failures. Always follow these ESD prevention procedures when removing and replacing modules:

- Ensure that the router chassis is electrically connected to the ground.
- Wear an ESD-preventive wrist strap, ensuring that it makes good skin contact. Connect the clip to an unpainted surface of the chassis frame to channel unwanted ESD voltages safely to ground. To guard against ESD damage and shocks, the wrist strap and cord must operate effectively.
- If no wrist strap is available, ground yourself by touching a metal part of the chassis.

Caution For the safety of your equipment, periodically check the resistance value of the anti-static strap. It should be between 1 and 10 megohms (Mohm).

General site requirements

This section describes the requirements your site must meet for the safe installation and operation of your router. Ensure that the site is properly prepared before beginning installation. If you are experiencing shutdowns or unusually high errors with your existing equipment, the guidelines provided in this section can also help you isolate the cause of failures and prevent future problems.

General precautions

Observe these general precautions when using and working with your Cisco 8300 Series Secure Routers:

- Keep your system components away from radiators and heat sources, and do not block cooling vents.
- Do not spill food or liquids on your system components, and never operate the product in a wet environment.
- Do not push any objects into the openings of your system components. Doing that can cause fire or electric shock by shorting out interior components.
- Position system cables and power supply cables carefully. Route system cables and the power supply cable and plug so that they cannot be stepped on or tripped over. Be sure that nothing else rests on your system component cables or power cable.
- Do not modify power cables or plugs. Consult a licensed electrician or your power company for electrical modifications at your site. Always follow your local and national wiring rules.
- If you turn off your system, wait at least 30 seconds before turning it on again to avoid system component damage.

Site selection guidelines

Cisco 8300 Series Secure Routers require specific environmental operating conditions. Temperature, humidity, altitude, and vibration can affect the performance and reliability of the router. The sections provide specific information to help you plan for the proper operating environment.

Site environmental requirements

Environmental monitoring in the router protects the system and components from damage caused by excessive voltage and temperature conditions. To ensure normal operation and avoid unnecessary maintenance, plan and prepare your site configuration before installation. After installation, ensure the site maintains the required environmental characteristics.

Table 6: Router environmental tolerances

Environmental Characteristic	Minimum	Maximum
Steady State Operating	0° C	For C8375-E-G2: 40° C at 10,000 feet
Short Term	-5° C	55° C at 6,000 feet
Storage	–40° C	+70° C
Humidity operating (noncondensing)	10%	90%
Humidity nonoperating (noncondensing)	5%	95%
Altitude operating: over allowable temperature range (0 to 40° C)	–500 feet	10,000 feet
Altitude, nonoperating: over allowable temperature range	–500 feet	60,000 feet
Thermal shock non-operating with12 mins	–40° C	+70° C

Note When mounting a Cisco 8300 Series Secure Router, the local ambient should be measured 2-inches from the I/O side of the product and, if possible, the local ambient should be measured 2-inches below the fully mounted product as well.

Physical characteristics

Be familiar with the physical characteristics of the Cisco 8300 Series Secure Routers to assist you in placing the system in the proper location.

For more information on the physical characteristics, see the datasheet for the Cisco 8300 Series Secure Routers.

Rack requirements

The Cisco 8300 Series Secure Routers include brackets for use with a 19-inch rack or, if specified in your order, optional larger brackets for use with a 23-inch rack.

These information can help you plan your equipment rack configuration:

- Allow clearance around the rack for maintenance.
- Enclosed racks must have adequate ventilation. Ensure that the rack is not congested, because each device generates heat. An enclosed rack should have louvered sides and a fan to provide cooling air. Heat generated by equipment at the bottom of the rack can be drawn upward into the intake ports of the equipment above it.
- If the chassis is installed on slides, check the position of the chassis when it is seated in the rack.

Note When mounting C8355-G2 on a rack, ensure at least one rack unit (1RU) of vertical space between routers. This ensures more heat removal, which in turn helps the local air temperature to stay within the specified operating conditions.

Router environmental requirements

Cisco 8300 Series Secure Routers can be placed on a desktop or installed in a rack. The location of your router and the layout of your equipment rack or wiring room are extremely important considerations for proper operation. Equipment placed too close together, inadequate ventilation, and inaccessible panels can cause malfunctions and shutdowns, and can make maintenance difficult. Plan for access to both front and rear panels of the router.

When planning your site layout and equipment locations, refer to the General Site Requirements section. If you are currently experiencing shutdowns or an unusually high number of errors with your existing equipment, these precautions and recommendations may help you to isolate the cause of failure and prevent future problems.

- Ensure that the room where your router operates has adequate air circulation. Electrical equipment generates heat. Without adequate air circulation, ambient air temperature may not cool equipment to acceptable operating temperatures.
- Always follow the ESD-prevention procedures to avoid damage to equipment. Damage from static discharge can cause immediate or intermittent equipment failure.
- Ensure that the chassis cover and module rear panels are secure. All empty network module slots, interface card slots, and power supply bays must have filler panels installed. The chassis is designed to allow cooling air to flow within it, through specially designed cooling slots. A chassis with uncovered openings permits air leaks, which may interrupt and reduce the flow of air across internal components.
- Baffles can help to isolate exhaust air from intake air. Baffles also help to draw cooling air through the chassis. The best placement of the baffles depends on the airflow patterns in the rack. You can find the best placement by experimenting with different configurations.

- When equipment installed in a rack (particularly in an enclosed rack) fails, try operating the equipment individually. Power off other equipment in the rack (and in adjacent racks) to allow the router under test maximum cooling air and clean power.

Power guidelines and requirements

Check the power at your site to ensure that you are receiving clean power (free of spikes and noise). Install a power conditioner if necessary.

The AC power supply includes these features:

- Autoselects either 110 V or 220 V operation.
- All units include a 6-foot (1.8-meter) electrical power cord. (A label near the power inlet indicates the correct voltage, frequency [only AC-powered systems], and current draw for the unit.)

For additional information on the power requirements, see the Cisco 8300 Series Secure Routers datasheet.

Network cabling specifications

The sections describe the cables required to install your Cisco 8300 Series Secure Routers:

Console port considerations

This device includes an asynchronous serial console port. You access to the device locally using a console terminal connected to the console port. This section discusses important cabling information that you must consider before connecting the device to a console terminal.

Flow control paces the transmission of data between a sending and a receiving device. Flow control ensures that the receiving device can absorb the data sent to it before the sending device sends more data. When the buffers on the receiving device are full, a message is sent to the sending device to suspend transmission until the data in the buffers is processed. Console terminals send data at speeds slower than the speeds modems do; therefore, the console port is ideally suited for use with console terminals.

Note Cisco 8300 Series Secure Routers have both EIA/TIA-232 asynchronous (RJ-45) and USB 5-pin mini Type B, 2.0 compliant serial console ports. Shielded USB cables with properly terminated shields are recommended.

EIA/TIA-232

Depending on the cable and the adapter used, this port appears as a DTE or DCE device at the end of the cable. At a time, only one port can be used.

The default parameters for the console port are 9600 baud, 8 data bits, 1 stop bit, and no parity. The console port does not support hardware flow control.

USB serial console

The USB serial console port connects directly to the USB connector of a PC. The console port does not support hardware flow control.

Note Always use shielded USB cables with a properly terminated shield.

The default parameters for the serial console port are 9600 baud, 8 data bits, no parity, and 1 stop bit.

No special drivers are needed for Mac OS X or Linux. At a time, only one console port can be active. When a cable is plugged into the USB console port, the RJ-45 port becomes inactive. Conversely, when the USB cable is removed from the USB port, the RJ-45 port becomes active.

Baud rates for the USB console port are 1200, 2400, 4800, 9600, 19200, 38400, 57600, and 115200 bps.

USB console OS compatibility

- Mac OS X version 10.5.4
- Redhat / Fedora Core 10 with kernel 2.6.27.5-117
- Ubuntu 8.10 with kernel 2.6.27-11
- Debian 5.0 with kernel 2.6
- Suse 11.1 with kernel 2.6.27.7-9

Note The Micro-USB type B serial port can be used as an alternative to the RJ-45 console port. For Windows operating systems earlier than Windows 7, you must install a Windows USB device driver before using the USB console port.

Prepare for network connections

When setting up your device, consider distance limitations and potential electromagnetic interference (EMI) as defined by the applicable local and international regulations.

Ethernet connections

The IEEE has established the Ethernet IEEE 802.3 Standards. The devices support the following Ethernet implementations:

- 1000BASE-T—1000 Mb/s full-duplex transmission over a Category 5 or better unshielded twisted-pair (UTP) cable. Supports the Ethernet maximum length of 328 feet (100 meters).
- 100BASE-T—100 Mb/s full-duplex transmission over a Category 5 or better unshielded twisted-pair (UTP) cable. Supports the Ethernet maximum length of 328 feet (100 meters).
- 10BASE-T—10 Mb/s full-duplex transmission over a Category 5 or better unshielded twisted-pair (UTP) cable. Supports the Ethernet maximum length of 328 feet (100 meters).

Required tools and equipment for installation and maintenance

⚠ **Warning** **Statement 1089—**Instructed and Skilled Person Definitions

An instructed person is someone who has been instructed and trained by a skilled person and takes the necessary precautions when working with equipment.

A skilled person or qualified personnel is someone who has training or experience in the equipment technology and understands potential hazards when working with equipment.

There are no serviceable parts inside. To avoid risk of electric shock, do not open.

⚠ **Warning** **Statement 1090—**Installation by Skilled Person

Only a skilled person should be allowed to install, replace, or service this equipment. See statement 1089 for the definition of a skilled person.

There are no serviceable parts inside. To avoid risk of electric shock, do not open.

⚠ **Warning** **Statement 1091—**Installation by an Instructed Person

Only an instructed person or skilled person should be allowed to install, replace, or service this equipment. See statement 1089 for the definition of an instructed or skilled person.

There are no serviceable parts inside. To avoid risk of electric shock, do not open.

You need the following tools and equipment to install and upgrade the router and its components:

- ESD-preventive cord and wrist strap
- Number 2 Phillips screwdriver
- Phillips screwdrivers: small, 3/16-in. (4 to 5 mm) and medium, 1/4-in. (6 to 7 mm)
  - To install or remove modules
  - To remove the cover, if you are upgrading memory or other components
- Screws that fit your rack
- Wire crimper
- Wire for connecting the chassis to an earth ground:
  - AWG 6 (13 mm²) wire for NEBS-compliant chassis grounding
  - AWG 14 (2 mm²) or larger wire for NEC-compliant chassis grounding
  - AWG 18 (1 mm²) or larger wire for EN/IEC 60950-compliant chassis grounding

- For NEC-compliant grounding, an appropriate user-supplied ring terminal, with an inner diameter of 1/4 in. (5 to 7 mm)

In addition, depending on the type of modules you plan to use, you might need the following equipment to connect a port to an external network:

- Cables for connection to the WAN and LAN ports (dependent on configuration)
- Ethernet hub or PC with a network interface card for connection to an Ethernet (LAN) port.
- Console terminal (an ASCII terminal or a PC running HyperTerminal or similar terminal emulation software) configured for 9600 baud, 8 data bits, 1 stop bit, no flow control, and no parity.
- Modem for connection to the auxiliary port for remote administrative access (optional).
- Data service unit (DSU) or channel service unit/data service unit (CSU/DSU) as appropriate for serial interfaces.
- External CSU for any CT1/PRI modules without a built-in CSU.

CHAPTER 3

Install and connect

This chapter describes how to install and connect the Cisco 8300 Series Secure Routers to LAN, WAN, and Voice networks.

Note These routers are designed to boot up in less than 30 minutes, provided the neighboring devices are in fully operational state.

Safety warnings

Warning To comply with Class A emissions requirements- shielded management Ethernet, CON, and AUX cables on the router must be used.

What you need to know

CLI console access

Use the USB or RJ-45 console port on the router to access the Cisco Internet Operating System (IOS-XE) and XE SD-WAN command line interface (CLI) on the router and perform configuration tasks. A terminal emulation program is required to establish communication between the router and a PC. See the Connect to a Console Terminal or Modem section in this document for instructions.

Note A Microsoft Windows USB driver must be installed before you establish physical connectivity between the router and the PC.

Software licenses

To use all the features on the router, you must purchase a software package. For more information on software licenses, see the “Smart Licensing” section of the Software Configuration Guide for the Cisco 8300 Series Secure Routers.

Before you begin

Before installing and connecting a Cisco 8300 Series Secure Routers, read the safety warnings and gather the following tools and equipment. For more information about the required tools and equipments, see the tools and equipment section.

CLI console access

Use the USB or RJ-45 console port on the router to access the Cisco Internet Operating System (IOS-XE) and XE SD-WAN command line interface (CLI) on the router and perform configuration tasks. A terminal emulation program is required to establish communication between the router and a PC. See the Connect to a console terminal or modem section in this document for instructions.

Note A Microsoft Windows USB driver must be installed before you establish physical connectivity between the router and the PC.

Software licenses

To use all the features on the router, you must purchase a software package. For more information on software licenses, see the “Smart Licensing” section of the Software Configuration Guide for the Cisco 8300 Series Secure Routers.

Unpack the device

Do not unpack the device until you are ready to install it. If the final installation site will not be ready for some time, keep the chassis in its shipping container to prevent accidental damage. When you are ready to install the chassis, proceed with unpacking it.

The chassis, accessory kit, publications, and any optional equipment you ordered may be shipped in more than one container. When you unpack the containers, check the packing list to ensure that you received all of the items on the list.

Install the device

If you need to install Network Interface Modules (NIMs), Service Modules (SMs), Pluggable Interface Modules (PIMs), and Field-Replaceable Units (FRUs) on the Cisco 8300 Series Secure Routers, you can install them either before or after you install the device. Ideally, you can install these modules when you have access to the I/O side of the device. Internal modules, memory cards and fan trays should be installed before rack-mounting the device.

You can install the device in one of the following ways:

- Set the chassis on a desktop
- Attach the chassis to the wall
- Mount the chassis on a rack

Note C8375-E-G2 support only rack mount, does not support wall mount or desktop mount options.

Caution To prevent damage to the chassis, do not attempt to lift or tilt the chassis by holding it by the plastic panel on the front. Always hold the chassis by the sides of the metal body.

Mount the chassis on a desktop

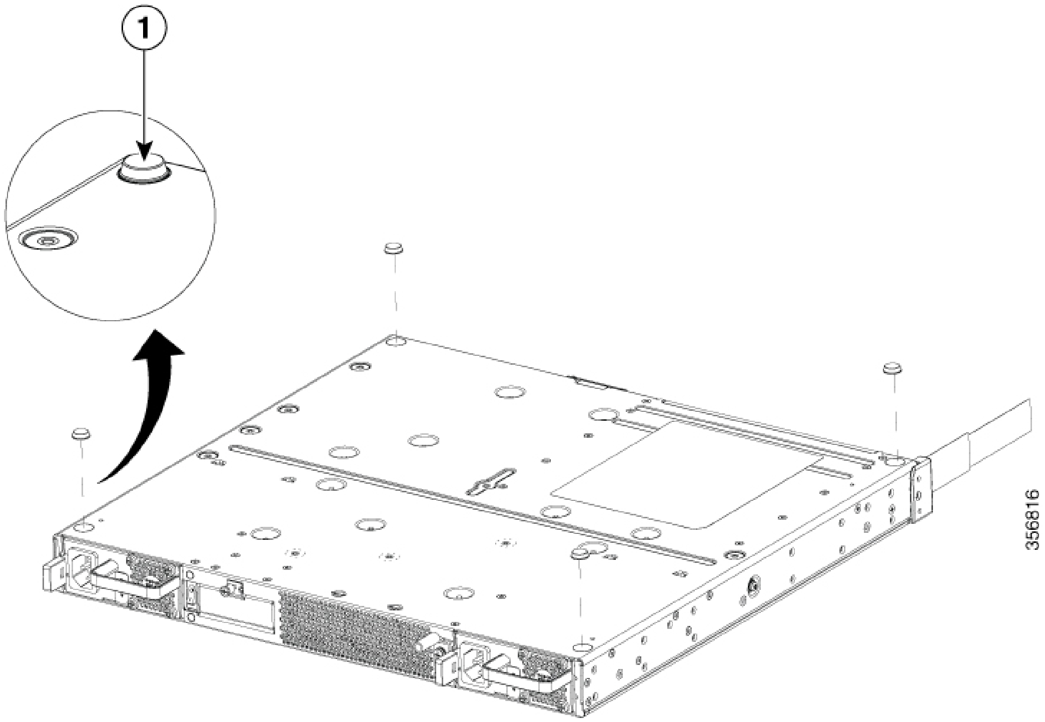
Warning **Statement 1032—**Lifting the Chassis

To prevent personal injury or damage to the chassis, never attempt to lift or tilt the chassis using the handles on modules, such as power supplies, fans, or cards. These types of handles are not designed to support the weight of the unit.

Step 1 Attach the elastomeric mount feet (label **1**) to the bottom of the device. The feet come with a pre-applied adhesive. Place the feet in the locations marked by a circle.

Step 2 You can place the device on a desktop, bench top, or shelf.

Figure 7: Feet adhesive on C8375-E-G2



Note Do not set the chassis in an area where the high acoustic noise can be an issue.

Caution Do not place anything on top of the device that weighs more than 10 pounds (4.5 kg), and do not stack device on a desktop. Excessive distributed weight of more than 10 pounds, or pound point load of 10 pounds on top could damage the chassis.

Caution Your chassis installation must allow unrestricted airflow for chassis cooling. For placing the device on a desktop, keep at least 1 inch (2.54 cm) of clear space beside the cooling inlet and exhaust vents.

After the device is installed, you must connect the chassis to a reliable earth ground. For the chassis ground connection procedures, see the Chassis Grounding section.

Rack mount the chassis

Warning **Statement 1024**—Ground Conductor

This equipment must be grounded. To reduce the risk of electric shock, never defeat the ground conductor or operate the equipment in the absence of a suitably installed ground conductor. Contact the appropriate electrical inspection authority or an electrician if you are uncertain that suitable grounding is available.

The Cisco 8300 Series Secure Routers can be installed in a 19-inch (48.26-cm) EIA and a 23-inch (58.42-cm) Southwestern Bell Corporation (SBC) racks. It can also be mounted in a 600-mm ETSI rack. Use the standard brackets shipped with the router for mounting the chassis in a 19-inch EIA rack; you can order optional larger brackets for mounting the chassis in a 23-inch SBC rack.

You can mount the devices in the following ways:

- Power Supply (PS) mounting—Brackets are attached at the PS side of the chassis with the front panel facing forward.
- Center-PS mounting—Brackets are attached in the centerof the chassis with the PS side facing forward.
- Center-I/O mounting—Brackets are attached in the center I/O side of the chassis with only the I/O side facing forward.
- I/O mounting—Brackets are attached at the I/O side of the chassis with the I/O side facing forward.

Attach the rack-mounting brackets

Caution Do not over-torque the screws. The recommended torque is 15 to 18 inch-lbs (1.7 to 2.0 N-m).

Caution Your chassis installation must allow unrestricted airflow for chassis cooling.

Attach the mounting brackets to the chassis as shown in the below figure using the screws provided. Use a #2 Philips screwdriver.

To attach the rack-mounting brackets to the device, perform these steps:

Procedure

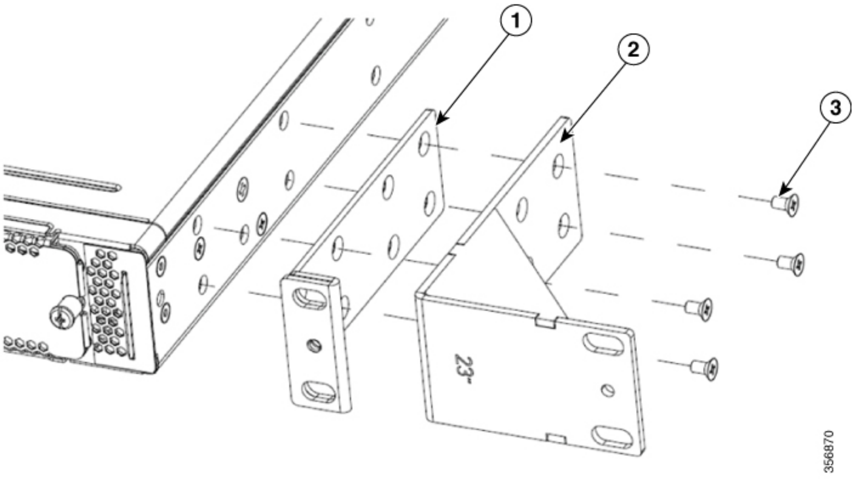
Step 1 Select the depth location for the router in the equipment rack. I/O side flush; I/O side recessed for the RFID badge; middle mount from the I/O side; middle mount from the power supply side; or power supply side flush.

Step 2 Align the rack mount bracket with the mounting holes in the side of the device.

Step 3 Insert the #6-32 FHM screws. Use only the screws that are provided in the rack mount bracket kit.

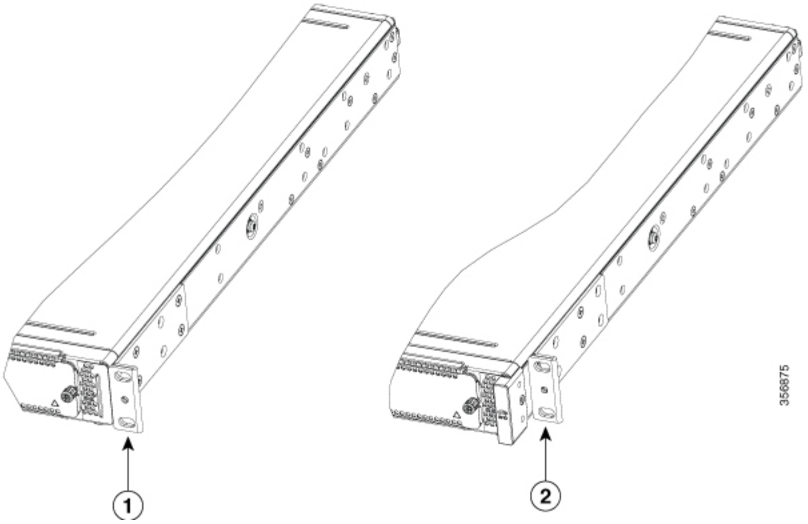
Step 4 Tighten the screws to a torque value of 15 to 18 inch-lb. (1.7 to 2.0 N-m).

Figure 8: Install brackets for I/O-side mounting (C8375-E-G2)



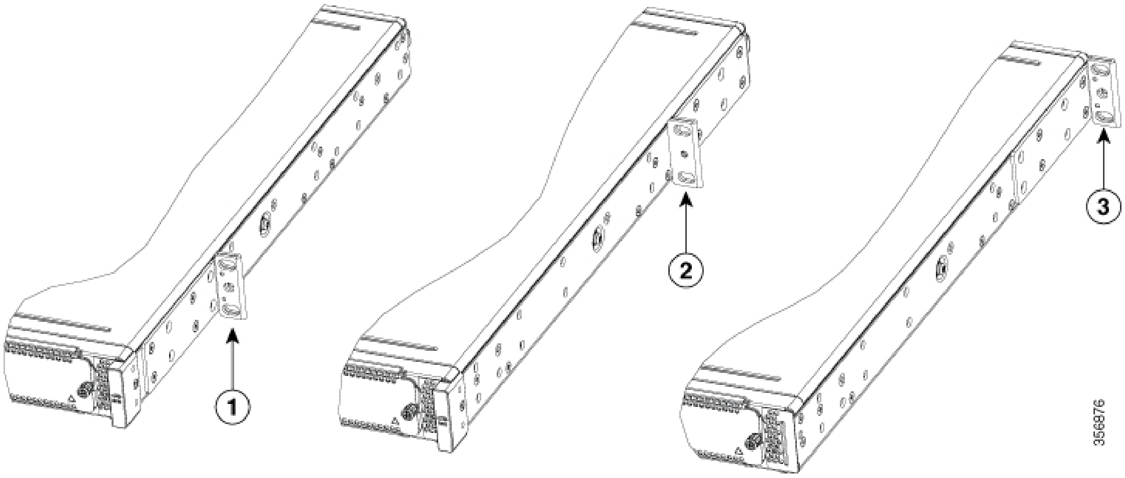
1	19-inch brackets
2	23-inch brackets
3	#6-32 PHMS

Figure 9: Rack mount bracket mounting positions



1	Flush with I/O side (No RFID)
2	I/O Side Recessed (for RFID)

Figure 10: Install brackets for PS mounting (C8375-E-G2)



1	Mid-Mount from Power Supply Side
2	Mid-Mount from I/O side
3	Power Supply Side Flush

Mount the chassis on a rack

After you attach the rack-mount brackets to the chassis, use screws to install the chassis onto the rack.

Tip For both the 19-inch EIA brackets and the 23-inch brackets, start the lower pair of screws first, and rest the brackets on the lower screws while you insert the upper pair of screws.

Tip The screw slots in the brackets are spaced to line up with every *second* pair of screw holes in the rack. When the correct screw holes are used, the small threaded holes in the brackets line up with unused screw holes in the rack. If the small holes do not line up with the rack holes, you must raise or lower the brackets to the next rack hole.

Warning To prevent bodily injury when mounting or servicing this unit in a rack, you must take special precautions to ensure that the system remains stable. The following guidelines are provided to ensure your safety:

- This unit should be mounted at the bottom of the rack if it is the only unit in the rack.
- When mounting this unit in a partially filled rack, load the rack from the bottom to the top with the heaviest component at the bottom of the rack.

⚠

Warning **Statement 1006—**Chassis Warning for Rack-Mounting and Servicing

To prevent bodily injury when mounting or servicing this unit in a rack, you must take special precautions to ensure that the system remains stable. The following guidelines are provided to ensure your safety:

- This unit should be mounted at the bottom of the rack if it is the only unit in the rack.
- When mounting this unit in a partially filled rack, load the rack from the bottom to the top with the heaviest component at the bottom of the rack.
- If the rack is provided with stabilizing devices, install the stabilizers before mounting or servicing the unit in the rack.

⚠

Warning **Statement 1032—**Lifting the Chassis

To prevent personal injury or damage to the chassis, never attempt to lift or tilt the chassis using the handles on modules, such as power supplies, fans, or cards. These types of handles are not designed to support the weight of the unit.

Figures below shows a typical rack mounting of a chassis in a rack.

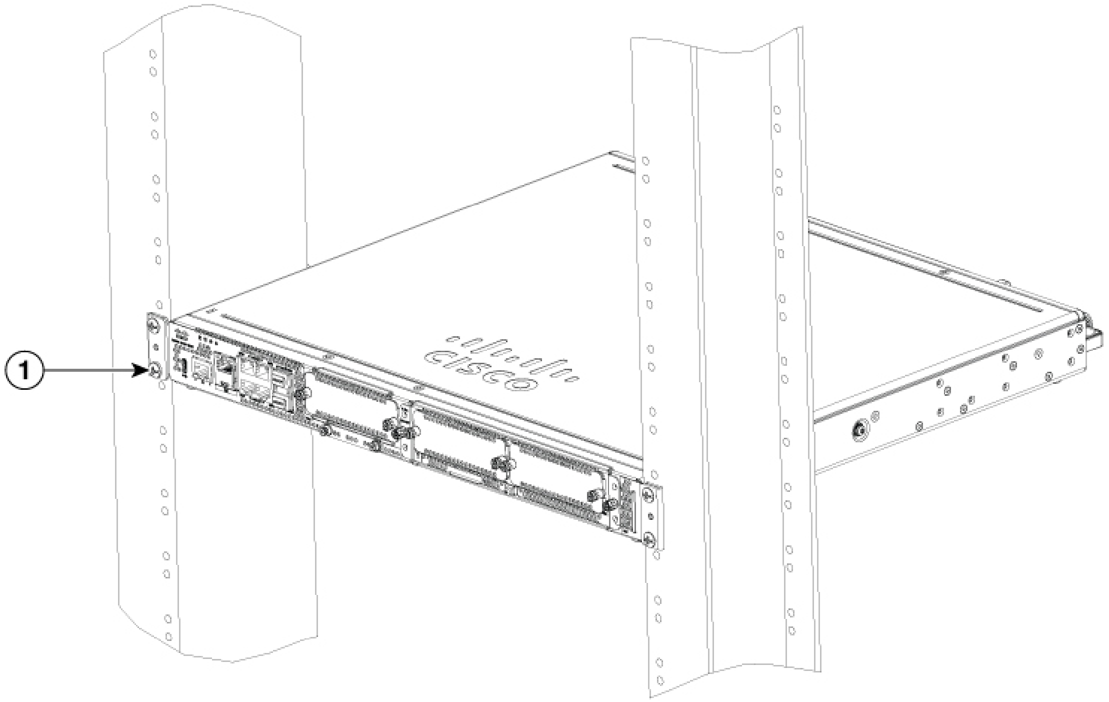
Step1. Locate the desired position in the equipment rack.

Step2. Align the holes in the rack mount brackets with the mounting holes in the equipment frame.

Step3. Secure the device using mounting screws appropriate for your equipment frame. The rack mount brackets have been designed #12-24 PHM screws.

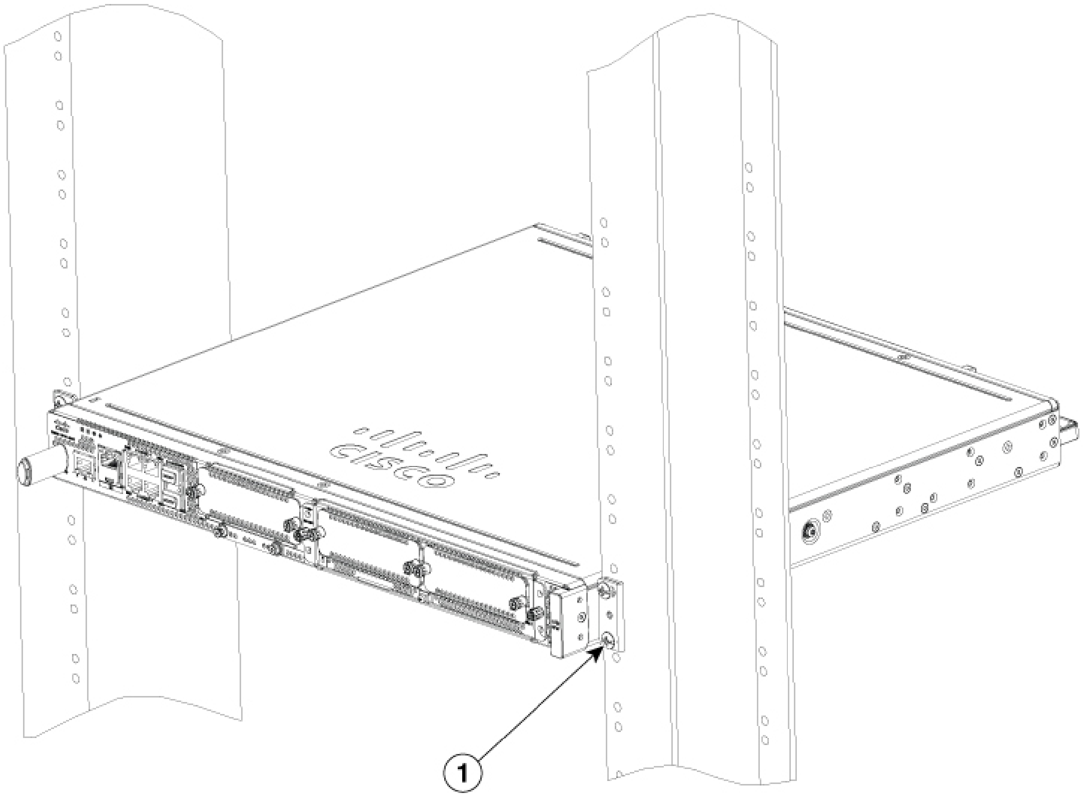
Step4. Tighten the screws to the appropriate torque value for your equipment

Figure 11: I/O flush mount, no RFID (C8375-E-G2)



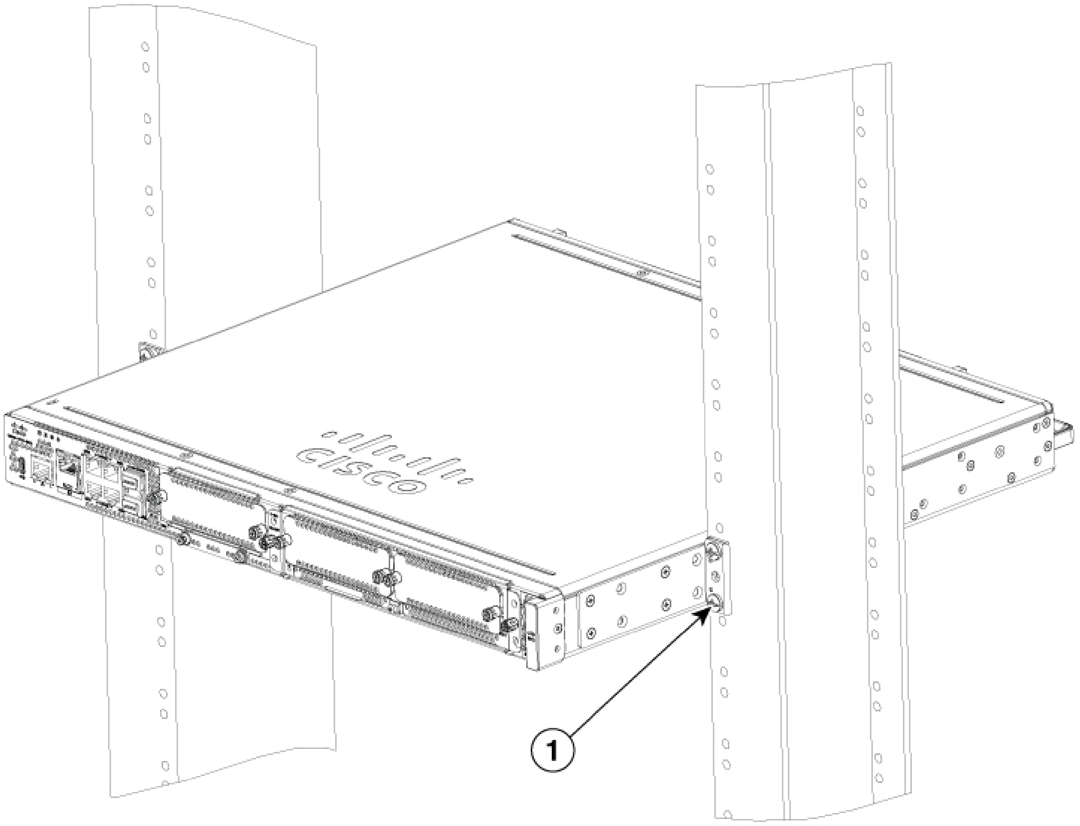
1	Rack Mounting screws

Figure 12: I/O mount with RFID (C8375-E-G2)



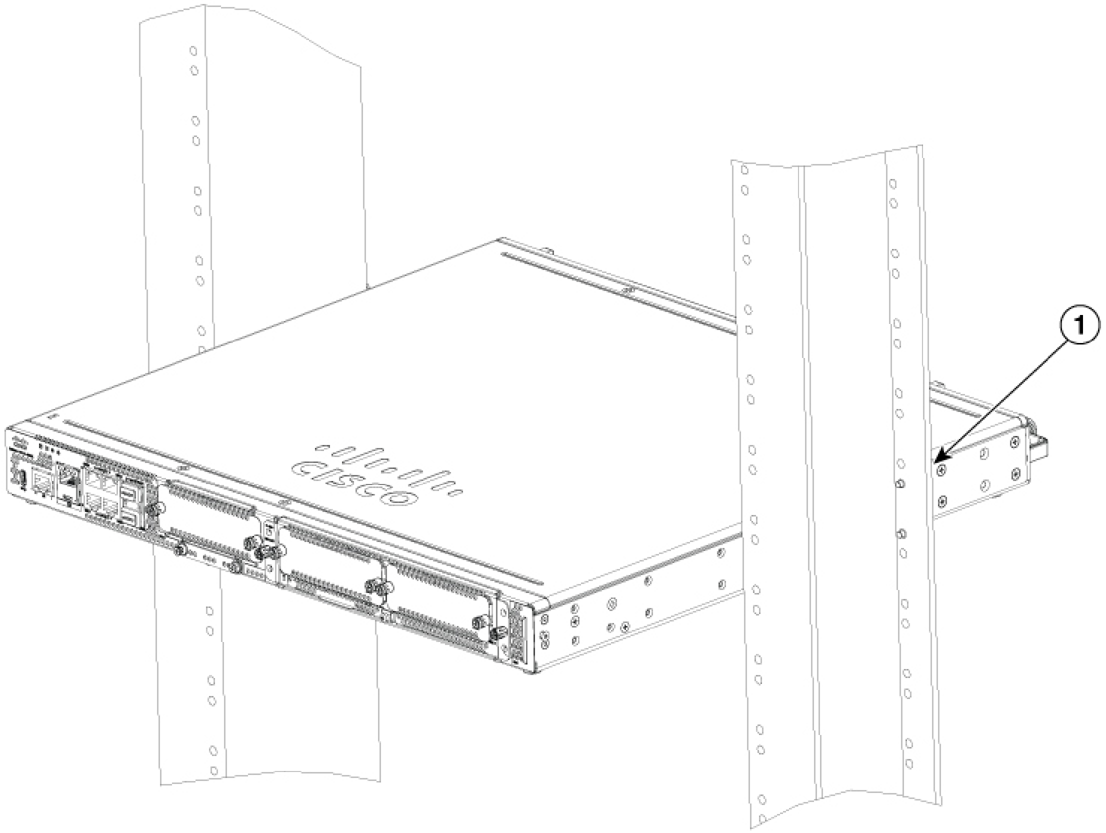
1	Rack Mounting screws

Figure 13: Mid mount from I/O Side (C8375-E-G2)



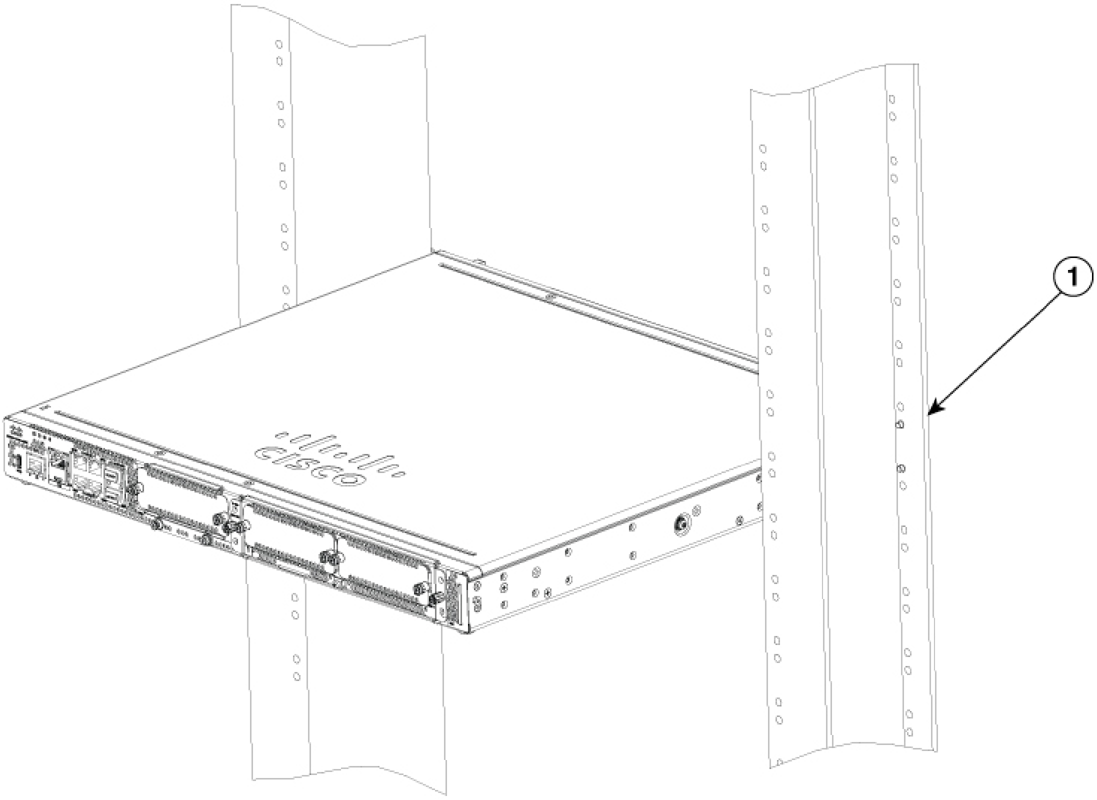
1	Rack Mounting screws

Figure 14: Mid-mount from power supply side (C8375-E-G2)



1	Rack Mounting screws

Figure 15: Power supply side-mount (C8375-E-G2)



1	Rack Mounting screws

Attach Cisco 8300 Series Secure Routers to a wall

Caution When mounted on a wall, the router should always be oriented with a side of the device oriented in the downward position. The I/O side and power supply side should be oriented so that the fan vents and cable entry will be oriented to the left or right. The I/O side or power supply should never be oriented downwards.

Caution Your chassis installation must allow unrestricted airflow for chassis cooling.

Wall mount C8375-E-G2

The steps provide information on attaching the wall mount brackets and how to wall mount the router.

Procedure

Step 1 Attach the rack mount brackets to the sides of the device using only the hardware provided in the wall mounting kit (#6-32 x 0.44 inch PHMS).

Step 2 The outer face of the rack mount bracket ear, the part that typically mounts to an equipment rack, should be placed against the side of the router. Use the spacers provided to adapt the larger obround holes down to smaller holes for the screws to fit into.

Step 3 The brackets should be located diagonally from each other as shown in the figure below.

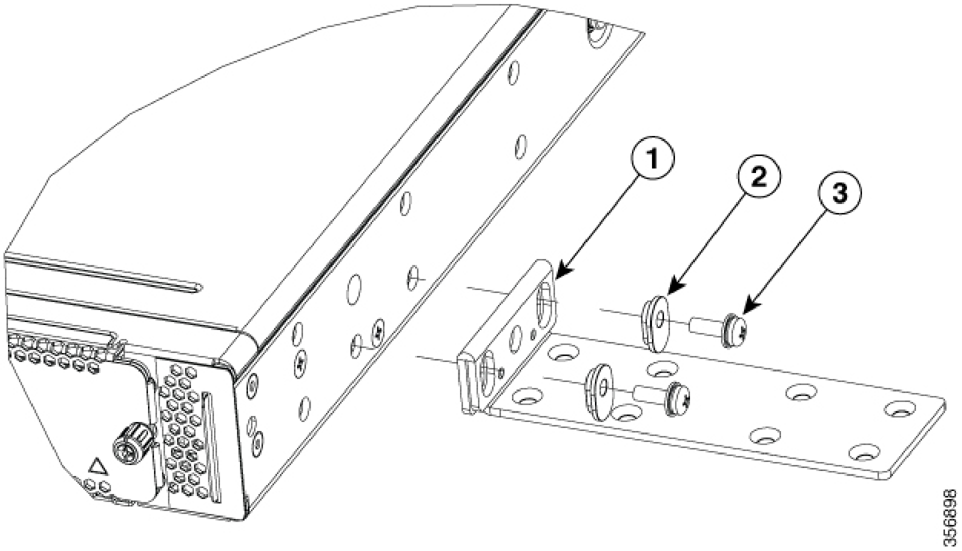
Step 4 Tighten the screws to a torque value of 15 to 18 inch-lb. (1.7 to 2.0 N-m).

Step 5 Use #6 or 4mm hardware to attach the brackets to the wall. At least 4 screws should be used per bracket, 8 screws in total. The screw length should be a minimum of 1 inch in length (25.4 mm).

Note
The customer supplies the appropriate hardware. Each mounting bracket has 8 holes that can be used for the mounting fasteners.

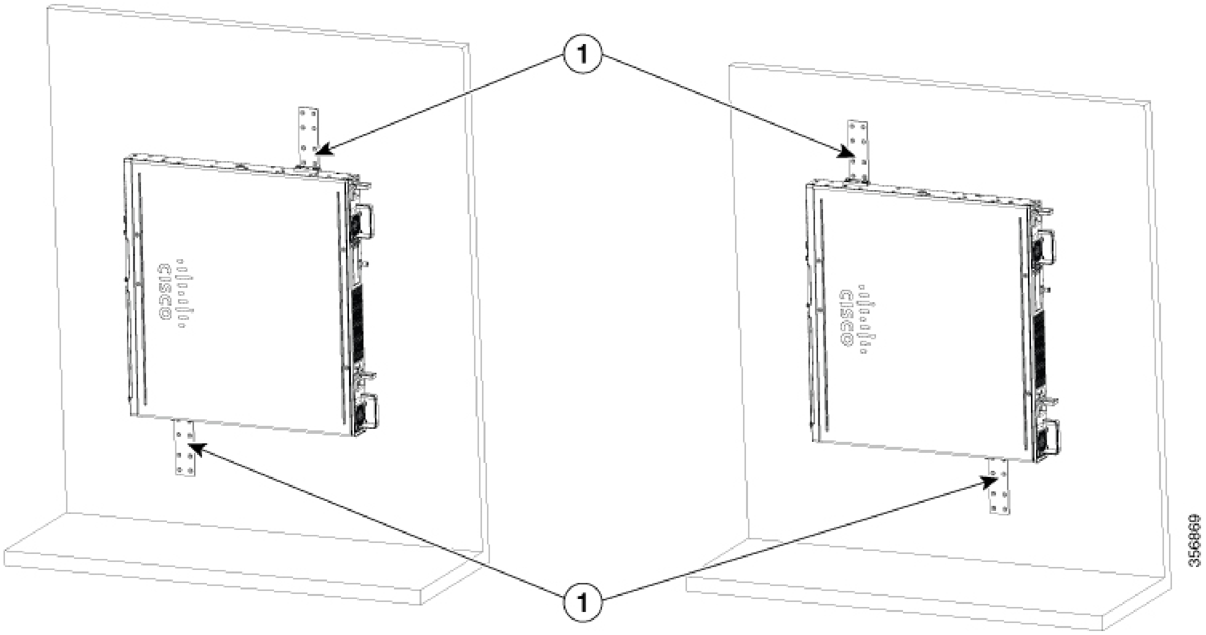
Step 6 Route the cables so that they do not put a strain on the connectors or mounting hardware.

Figure 16: Attach Wall Mount Brackets (C8375-E-G2)



1	19-inches bracket
2	Plastic spacer
3	#6-32 PHMS

Figure 17: Wall Mount the C8375-E-G2



1	Customer supplied wall mount hardware

Ground the chassis

After the device is installed, you must connect the chassis to a reliable earth ground.

Chassis grounding

Warning **Statement 1024**—Ground Conductor

This equipment must be grounded. To reduce the risk of electric shock, never defeat the ground conductor or operate the equipment in the absence of a suitably installed ground conductor. Contact the appropriate electrical inspection authority or an electrician if you are uncertain that suitable grounding is available.

You must connect the chassis to a reliable earth ground; the ground wire must be installed in accordance with local electrical safety standards.

- For grounding, use size 6 AWG (13 mm^2) copper wire and the ground lug provided in the accessory kit.

Note This equipment is suitable for installation in Network Telecommunications Facilities and locations where the NEC applies. The equipment is suitable for installation as part of the Common Bonding Network (CBN).

- For NEC-compliant grounding, use size 14 AWG (2 mm²) or larger copper wire and an appropriate user-supplied ring terminal with an inner diameter of 1/4 in. (5–7 mm)
- AWG 10 (4 mm²) or larger wire for EN/IEC 60950-1 and EN/IEC 62368-1 compliant chassis grounding

Note The grounding wire should be sized according to local and national installation requirements. The above recommended AWG values for NEBS-compliant, NEC-compliant, EN/IEC 60950-1 and EN/IEC 62368-1 as the minimum requirement respectively, the higher AWG value recommendation also with the higher priority, this means AWG 10 is the minimum requirement only when NEBS is not required. Commercially available 6-AWG grounding wire is always preferred from the chassis to the rack ground or directly to the common bonding network (CBN). The length of the grounding wire depends on the proximity of the switch to proper grounding facilities.

To install the ground connection for your device, perform the following steps:

Procedure

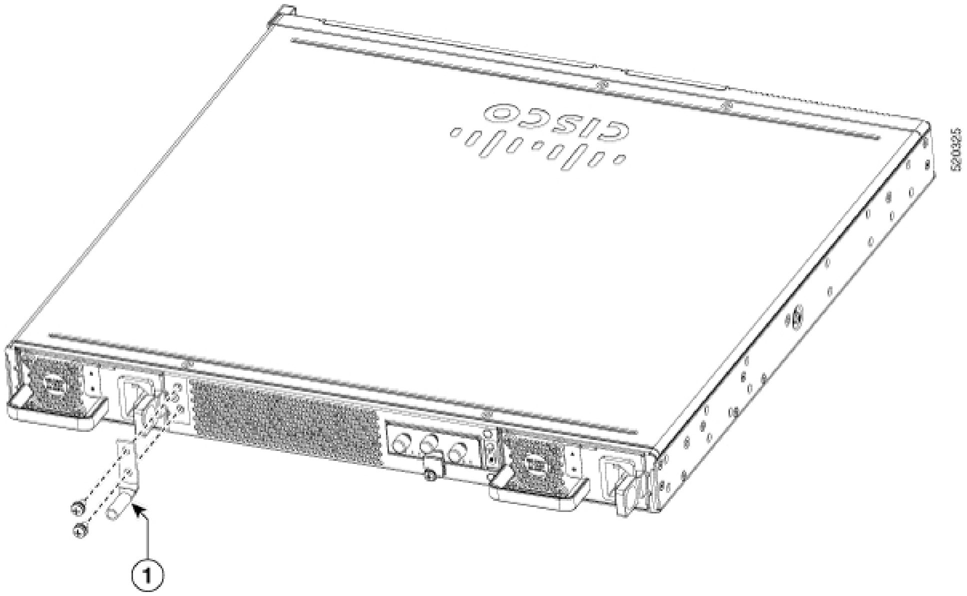
Step 1 Strip one end of the ground wire to the length required for the ground lug or terminal.

- For the ground lug—approximately 0.75 inch (20 mm)
- For user-provided ring terminal—as required

Step 2 Crimp the ground wire to the ground lug or ring terminal, using a crimp tool of the appropriate size.

Step 3 Attach the ground lug or ring terminal to the chassis as shown in Chassis Grounding section. For a ground lug, use the two screws with captive locking washers provided. For a ring terminal, use one of the screws provided. Tighten the screws to a torque of 8 to 10 in-lb (0.9 to 1.1 N-m).

Figure 18: Chassis ground connection on the C8375-E-G2



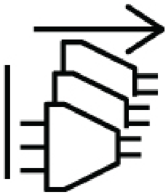
Step 4 Connect the other end of the ground wire to a known reliable earth ground point at your site.

Connect power to the device

This section explains how to connect power to the device.

Warning **Statement 1028—**More Than One Power Supply

This unit might have more than one power supply connection. To reduce risk of electric shock, remove all connections to de-energize the unit.



Note The installation must comply with all required electrical codes applicable at the installation site.

If your device uses AC power, connect it to a 15 A, 120 VAC (10 A, 240 VAC) circuit with overcurrent protection.

Note The input voltage tolerance limits for AC power are 90 and 264 VAC.

Note This product requires surge protection to be provided as part of the building installation. To comply with the Telcordia GR-1089 NEBS standard for electromagnetic compatibility and safety, an external surge protective device (SPD) is required at the AC power service equipment.

Warning **Statement 1005**—Circuit Breaker

This product relies on the building's installation for short-circuit (overcurrent) protection. To reduce risk of electric shock or fire, ensure that the protective device is rated not greater than: 20A.

Connect to a console terminal or modem

The Cisco 8300 Series Secure Routers have asynchronous serial ports. These ports provide administrative access to the router either locally (with a console terminal or a PC).To configure the router through the Cisco IOS CLI, you must establish a connection between the router console port and either a terminal or a PC.

Use these cables and adapters to establish a local or remote connection.

Figure 19: Ports for C8375-E-G2

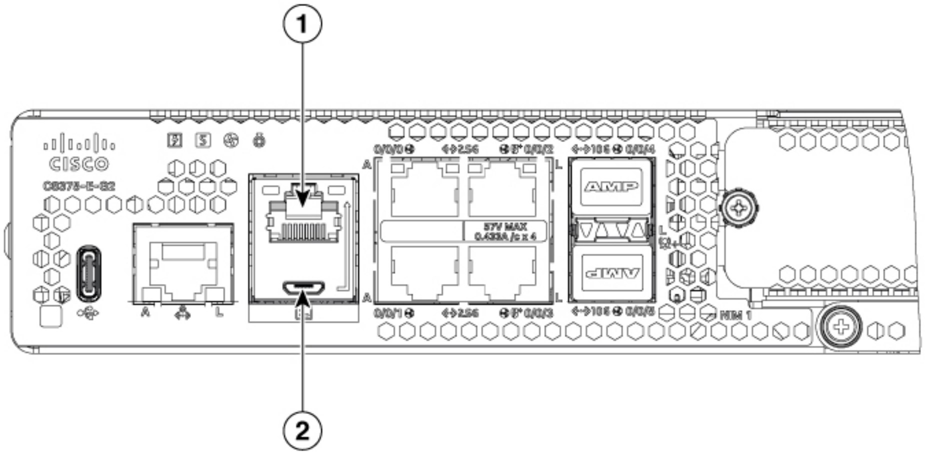


Table 7: Local and remote connections for C8375-E-G2

Port Type	Cable	Section
1. Serial (RJ-45)	EIA RJ-45	Connect to the Serial Port with Microsoft Windows
2. Serial (USB)	USB 5-pin mini USB Type-B-to-USB Type-A	

Connect to the console port with Mac OS X

This procedure describes how to connect a Mac OS X system USB port to the console using the built in OS X Terminal utility.

Procedure

Step 1 Use the Finder to go to Applications > Utilities > Terminal.

Step 2 Connect the OS X USB port to the router.

Step 3 Enter the commands to find the OS X USB port number

Example:

```
macbook:user$ cd /dev
macbook:user$ ls -ltr /dev/*usb*
crw-rw-rw-  1 root    wheel       9,  66 Apr  1 16:46 tty.usbmodem1a21 DT-macbook:dev user$
```

Step 4 Connect to the USB port with the command followed by the router USB port speed

Example:

```
macbook:user$ screen /dev/tty.usbmodem1a21 9600
```

To disconnect the OS X USB console from the terminal window

Enter Ctrl-a followed by Ctrl-\

Connect to the console port with Linux

This procedure shows how to connect a Linux system USB port to the console using the built in Linux Terminal utility.

Procedure

Step 1 Open the Linux Terminal window.

Step 2 Connect the Linux USB port to the router.

Step 3 Enter the commands to find the Linux USB port number

Example:

```
root@usb-suse# cd /dev
root@usb-suse /dev# ls -ltr *ACM*
crw-r--r--    1 root     root     188,   0 Jan 14 18:02 ttyACM0
root@usb-suse /dev#
```

Step 4 Connect to the USB port with the command followed by the router USB port speed

Example:

```
root@usb-suse /dev# screen /dev/ttyACM0 9600
```

To disconnect the Linux USB console from the Terminal window

Enter Ctrl-a followed by : then quit

Install the Silicon Labs USB device driver

This section contains these topics:

Install the Silicon Labs Windows USB device driver

Procedure

Step 1 Go to the Silicon Labs website (www.silabs.com/developers/usb-to-uart-bridge-vcp-drivers?tab=downloads), and click CP210x Universal Windows Driver.

Step 2 Unzip the downloaded folder, and select the installer for your system configuration. The Device Driver Installation Wizard begins.

Step 3 Click Next on the Installation Wizard, then click Finish to complete installation.

Step 4 Open the Device Manager on your system and click the Ports (COM & LPT) drop-down.

Step 5 Insert the USB console cable and power into your system. The Device manager refreshes and indicates the newly-detected COM port.

Step 6 Open a terminal emulator and click the Serial connection type. Input the values for Serial Line and Speed (or Baud Rate).

Step 7 Click Open.

Step 8 The terminal emulator opens. Click Enter to view the console output response.

The USB console is ready for use.

Install the Silicon Labs Mac USB device driver

Procedure

Step 1 Go to the Silicon Labs website (www.silabs.com/developers/usb-to-uart-bridge-vcp-drivers?tab=downloads), and click CP210x VCP Mac OSX Driver.

Step 2 Click the Downloads folder, then click the macOS_VCP_Driver folder, and double-click the SiLabsUSBDriverDisk.dmg program.

Step 3 Click Install CP210X VCP Driver, and then click Open. The Driver Installer begins.

Step 4 Follow installer instructions. Click Continue, scroll all the way down, then click Continue, and click Agree.

Step 5 Click Continue, and enter your password. Then click Install Helper, and click Close.

Step 6 Insert the USB console cable and power into your system..

Step 7 Open a terminal and type cd/dev, and then type ls-ltr. Serial port tty.SLAB_USBtoUART appears.

Step 8 Type screen/dev/tty.SLAB_USBtoUART <baudrate> to see console output. Console will show response upon first Enter key if there is no output.

The USB console is ready for use.

Connect WAN and LAN interfaces

This section describes how to connect WAN and LAN interface cables.

Ports and cables

The connections summarized here are also described in detail in the document on Cisco Modular Access Cable Specifications .

Table 8: WAN, LAN, and Voice connections

Port or Connection	Port Type, Color[1]	Connection:	Cable
Ethernet	RJ-45, yellow	Ethernet hub or Ethernet switch	Category 5 or higher Ethernet
T1/E1 WANxCE1T1-PRI	RJ-48C/CA81ARJ-48S, tan	T1 or E1 networkExternal T1 CSU or other T1 equipment	RJ-48 T1/E1RJ-48S to RJ-48S TERJ-48S to RJ-48S NTRJ-48S to RJ-48S T1RJ-48S to bareRJ-48S to BNCRJ-48S to twinaxial cableRJ-48S to DB-15RJ-48S to DB-15 null
T3/DS3/E3 WAN	BNC connector	T3 network, CSU/DSU, or other T3/DS3 equipment	75-ohm coaxial cable
Cisco serial	60-pin D-sub, blue	CSU/DSU and serial network or equipment	Cisco serial transition cable that matches the signaling protocol (EIA/TIA-232, EIA/TIA-449, V.35, X.21, or EIA-530) and the serial port operating mode (DTE or DCE).[2]
Cisco Smart serial	Cisco Smart compact connector, blue	CSU/DSU and serial network or equipment	
Gigabit Ethernet SFP, optical	LC, color according to optical wavelength	1000BASE-SX, -LX, -LH, -ZX, -CWDM	Optical fiber as specified on applicable data sheet
Gigabit Ethernet SFP, copper	RJ-45	1000BASE-T	Category 5, 5e, 6 UTP
Gigabit Ethernet SFP+, optical	LC, color according to optical wavelength	10G-SR, -LR, -ER, -DWDM,-AOC,-CU	Optical fiber as specified on applicable data sheet
Gigabit Ethernet SFP+, copper	RJ-45	10GBASE-T	Category 6, Category 7

[1] Cable color codes are specific to Cisco cables.

[2] See the Cisco Modular Access Router Cable Specifications document for information about choosing these cables.

Connection procedures and precautions

- Connect each WAN and LAN to the appropriate connector on the chassis or on a network module or interface card.

- Position the cables carefully, so that they do not put strain on the connectors.
- Organize cables in bundles so that cables do not intertwine.
- Inspect the cables to make sure that the routing and bend radius is satisfactory. Reposition cables, if necessary.
- Install cable ties in accordance with site requirements.

For cable pinouts, see Cisco Modular Access Cable Specifications.

Note After installing the device and connecting the cables, you can configure the device with basic configurations. For more information on how to configure the device, see the Cisco 8300 Series Secure Routers Software Configuration Guide.

CHAPTER 4

Install internal components and field replaceable units

This document describes how to install internal components and field replaceable units (FRUs) in the Cisco 8300 Series Secure Routers. The installation information is contained in these sections:

Safety warnings

Warning **Statement 1100—**Before Making Telecommunication Network Connection

High touch/leakage current—Permanently connected protective earth ground is essential before connecting to the telecommunication network.

Warning **Statement 1008—**Class 1 Laser Product

This product is a Class 1 laser product.

Warning **Statement 445—**Connect the Chassis to Earth Ground

To reduce the risk of electric shock, connect the chassis of this equipment to permanent earth ground during normal use.

Warning **Statement 1022—**Disconnect Device

To reduce the risk of electric shock and fire, a readily accessible disconnect device must be incorporated in the fixed wiring.

Warning **Statement 1051—**Laser Radiation

Invisible laser radiation may be emitted from disconnected fibers or connectors. Do not stare into beams or view directly with optical instruments.

Warning **Statement 1056—**Unterminated Fiber Cable

Invisible laser radiation may be emitted from the end of the unterminated fiber cable or connector. Do not view directly with optical instruments. Viewing the laser output with certain optical instruments, for example, eye loupes, magnifiers, and microscopes, within a distance of 100 mm, may pose an eye hazard.

Warning **Statement 1089—**Instructed and Skilled Person Definitions

An instructed person is someone who has been instructed and trained by a skilled person and takes the necessary precautions when working with equipment.

A skilled person or qualified personnel is someone who has training or experience in the equipment technology and understands potential hazards when working with equipment.

There are no serviceable parts inside. To avoid risk of electric shock, do not open.

Warning **Statement 1090—**Installation by Skilled Person

Only a skilled person should be allowed to install, replace, or service this equipment. See statement 1089 for the definition of a skilled person.

There are no serviceable parts inside. To avoid risk of electric shock, do not open.

Warning **Statement 1091—**Installation by an Instructed Person

Only an instructed person or skilled person should be allowed to install, replace, or service this equipment. See statement 1089 for the definition of an instructed or skilled person.

There are no serviceable parts inside. To avoid risk of electric shock, do not open.

Warning **Statement 1255—**Laser Compliance Statement

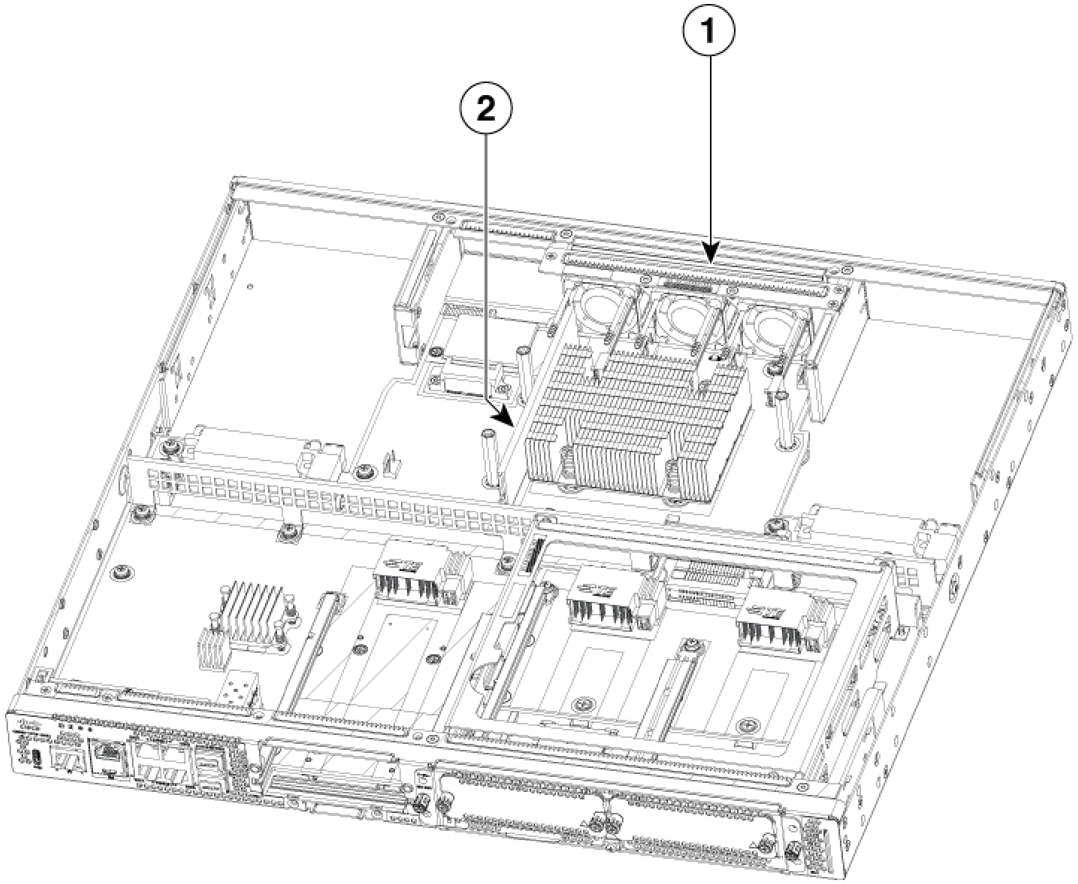
Pluggable optical modules comply with IEC 60825-1 Ed. 3 and 21 CFR 1040.10 and 1040.11 with or without exception for conformance with IEC 60825-1 Ed. 3 as described in Laser Notice No. 56, dated May 8, 2019.

Locate and access internal components

The figure shows the locations of internal components on the motherboard. Internal modules include DIMMs on Cisco 8300 Series Secure Routers.

To access the internal components on the device, you must first remove the chassis cover. For instructions on how to remove and replace the chassis cover on the device, see the sections on Install and Remove Chassis Covers.

Figure 20: Internal component locations in the C8375-E-G2



Sl. No	Modules
1	Fan tray
2	DIMM

Remove and replace the chassis cover

The Cisco 8300 Series Secure Routers have removable covers. Before removing the cover, do these steps:

- Do not run the device with the cover off. Doing so can cause the chassis to overheat very quickly.
- Disconnect all power cables.
- Remove the device from the rack

Warning **Statement 1041—**Disconnect Telephone Network Cables

Before opening the unit, disconnect the telephone network cables to avoid contact with telephone network voltages.

Use a number-2 Phillips screwdriver to perform these tasks.

Remove the chassis cover

To remove the cover, perform the following steps.

Procedure

Step 1 Read the Safety Warnings and disconnect the power supply before you perform any module replacement.

Step 2 Confirm the device is turned off and disconnected from the power supply or power supplies. If a redundant power is used, disconnect from the redundant power supply.

Step 3 Place the chassis on a flat surface.

Step 4 Remove the 11 cover screws.

Step 5 Lift the cover straight up.

Replace the cover

To replace the cover, perform these steps.

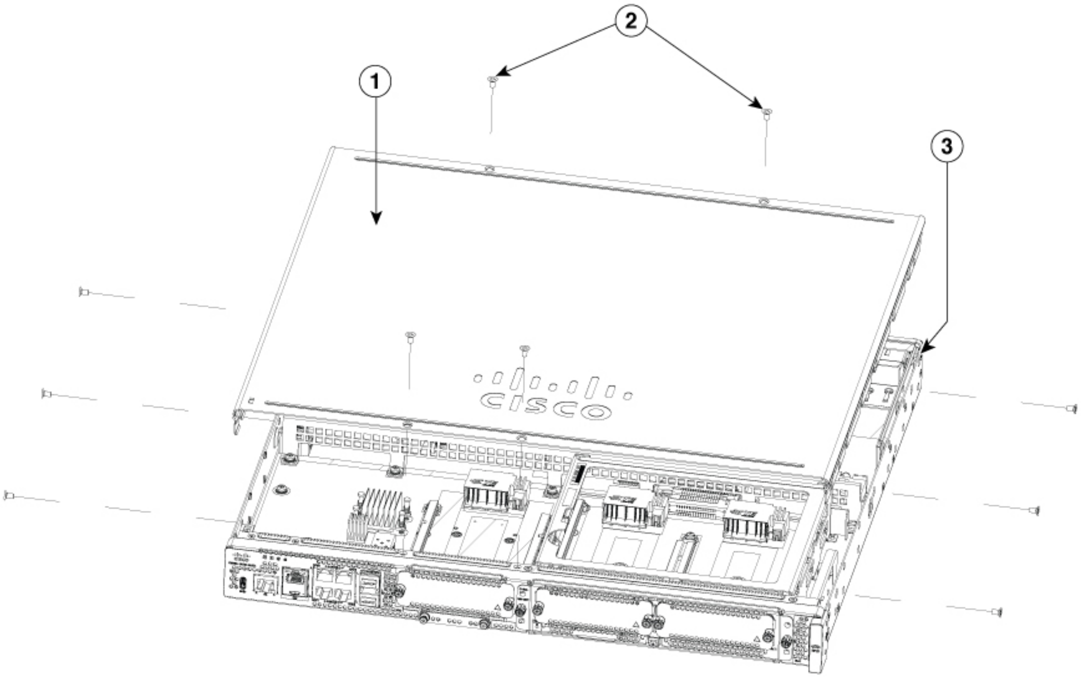
Procedure

Step 1 Place the chassis on a flat surface.

Step 2 Drop the cover straight down and ensure that the side flanges insert into the chassis. Care should be taken to not damage the EMC Gaskets.

Step 3 Install the 11 cover screws.

Figure 21: Install the cover on the C8375-E-G2



1	Chassis cover
2	Screws
3	Chassis

Remove and replace DDR DIMMs

To access the DIMMs, you must remove the chassis cover as described in the Access and Install Modules section.

⚠

Caution Always wear an ESD-preventive wrist strap and ensure that it makes good contact with your skin when you remove or install DIMMs. Connect the equipment end of the wrist strap to the metal part of the chassis.

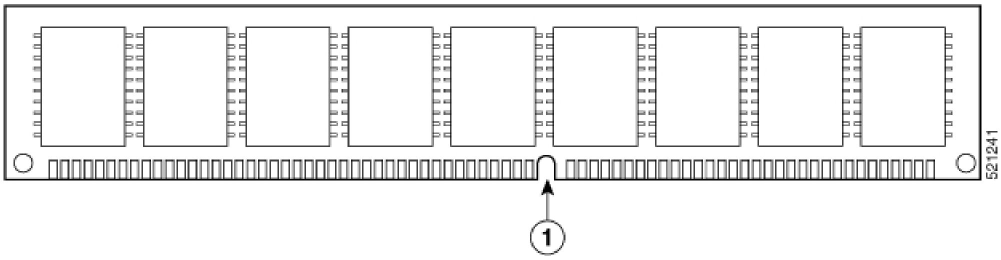
⚠

Caution Handle DIMMs by the edges only. DIMMs are ESD-sensitive components and can be damaged by mishandling.

Locate and orient DIMM

DIMMs have a polarization notch on the mating edge to prevent incorrect insertion. The image shows the polarization notch on a DIMM.

Figure 22: DIMM Showing Polarization Notch



1	Polarization notch

Remove a DIMM

Follow these steps to remove a DIMM:

Procedure

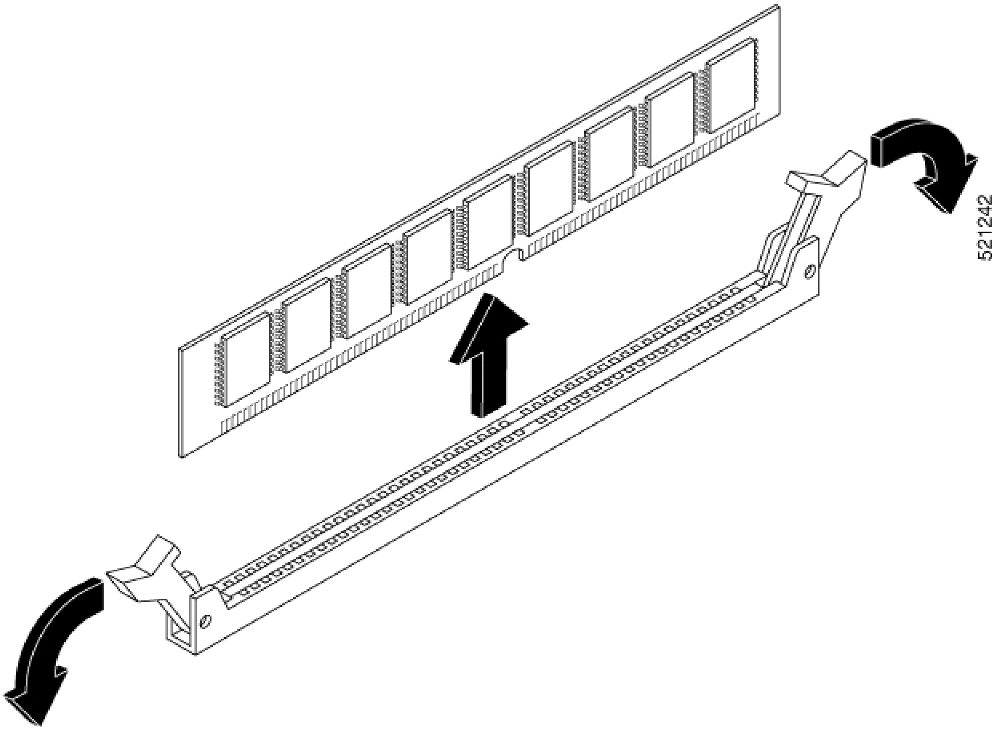
Step 1 Read the Safety Warnings section and disconnect the power supply before you perform any module replacement.

Step 2 If the cover is not already removed, remove the chassis cover.

Step 3 Locate the DIMM module to find the DIMM sockets on the chassis.

Step 4 Rotate DIMM connector handles downwards to extract the DIMM module.

Figure 23: Remove a DIMM



Install a DIMM

Follow these steps to install a DIMM on the Cisco 8300 Series Secure Routers.

Procedure

Step 1 Read the Safety Warnings section and disconnect the power supply before you perform any DIMM replacement.

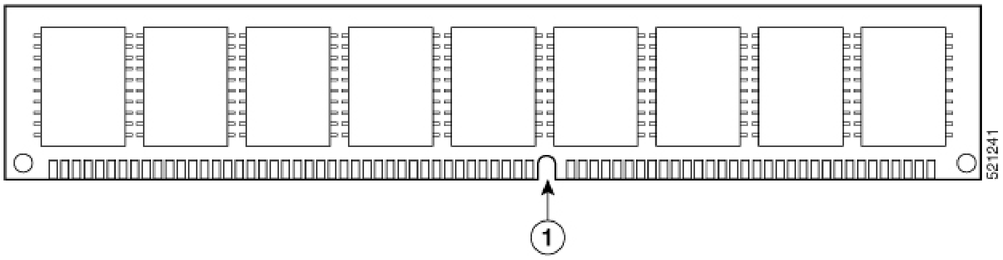
Step 2 If the cover is not already removed, remove the chassis cover.

Step 3 Locate the DIMM module to find the DIMM sockets on the device.

Step 4 Ensure that both latches on the DIMM connector are in the open position.

Step 5 Orient the DIMM so that the polarization notch lines up with the polarization key on the connector.

Figure 24: DIMM showing Polarization Notch

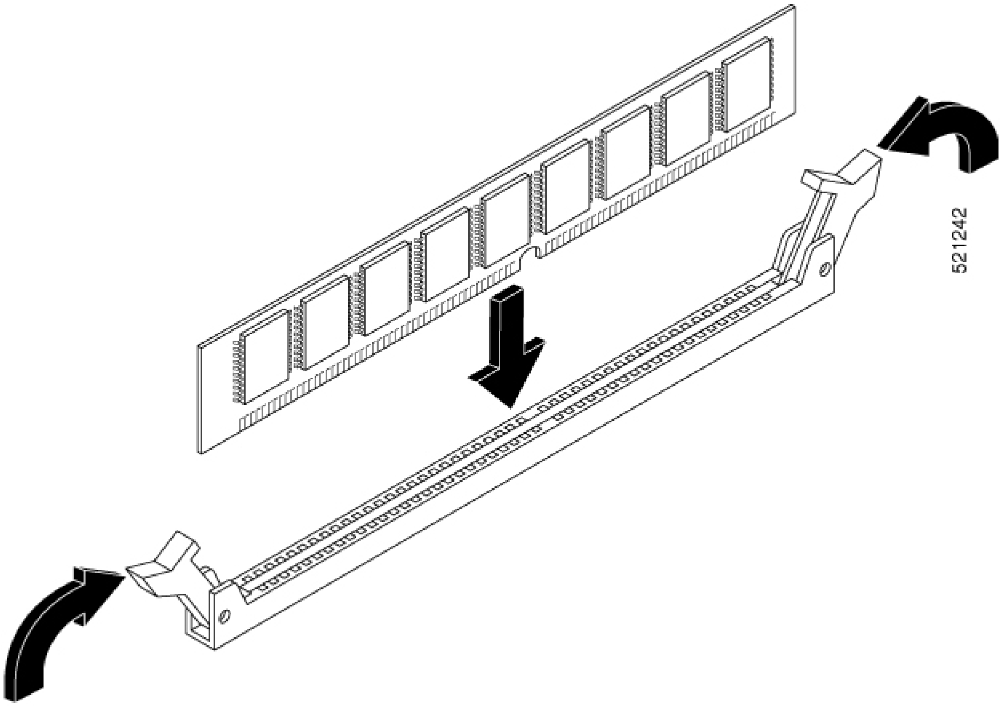


Step 6 Insert the DIMM into the connector one side at a time.

Step 7 Rotate the connector handles upward and click into place.

Step 8 Reinstall the chassis cover.

Figure 25: Install a DIMM



Step 9 Replace the chassis cover.

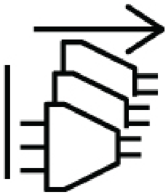
Remove and replace the power supplies

Warning **Statement 1029—**Blank Faceplates and Cover Panels

Blank faceplates and cover panels serve three important functions: they reduce the risk of electric shock and fire, 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.

Warning **Statement 1028—**More Than One Power Supply

This unit might have more than one power supply connection. To reduce risk of electric shock, remove all connections to de-energize the unit.



Warning Care should be taken while removing the power supplies (especially in boost mode of operation). If the total power consumption is higher than can be supported by one power supply alone and in this condition a power supply is removed, the hardware can be damaged. This may then result in the system being unstable or unusable.

AC power supplies

The Cisco 8300 Series Secure Routers device have two different AC power supply types and they are the same physical size. The power supplies cannot be interchanged.

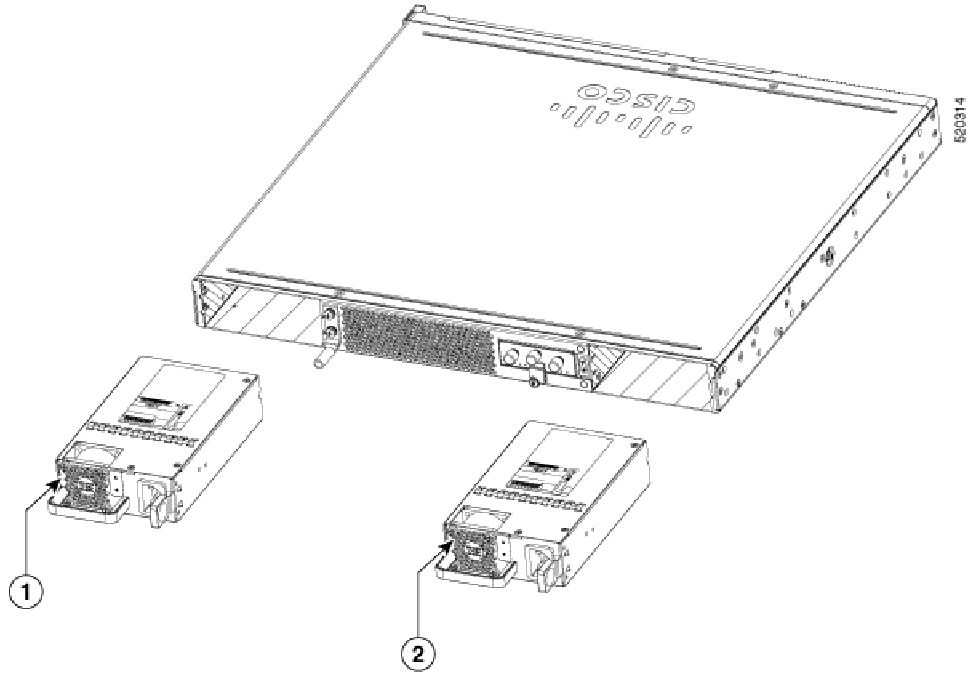
Overview of the AC power supply

The AC power supplies for the Cisco 8300 Series Secure Routers device are:

- PWR-CC1-400WAC
- PWR-CC1-760WAC

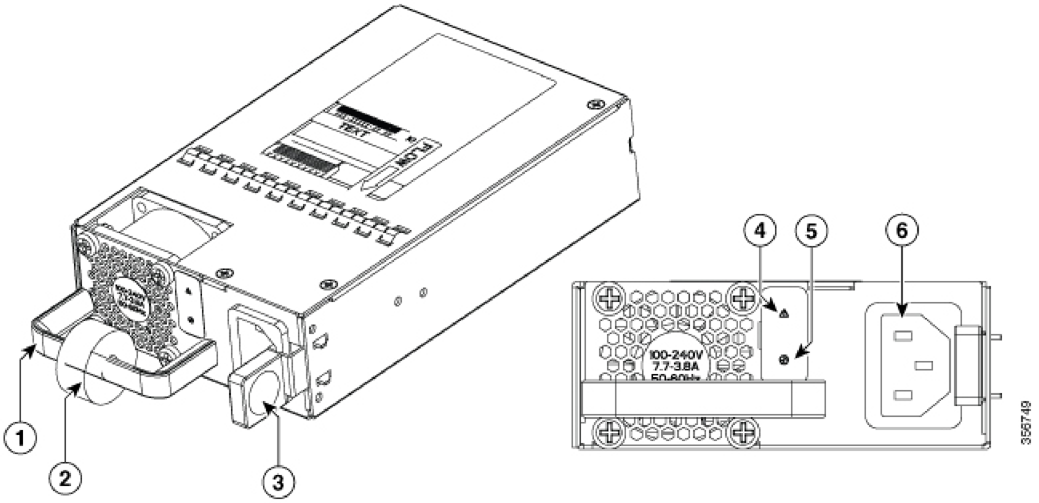
The two supplies are physically similar and a diagram is shown in this figure.

Figure 26: 400W AC power supply for C8375-E-G2



Sl. No	Module
1	PSU1
2	PSU0

Figure 27: 760W AC power supply for C8375-E-G2



1	Handle	2	Strain relief

3	Latch	4	Fail LED
5	Status LED	6	Power socket

Remove and replace the AC power supply

To remove an AC power supply from the Cisco 8300 Series Secure Routers, perform these steps:

Procedure

Step 1 Read the safety warnings section of this document.

Step 2 If there is only one power supply in the system, shut down the device before removing the power supply.

Step 3 If there are redundant power supplies in use the device does not have to be shut down prior to replacing the power supply. The power supply may be replaced while the device is in service.

Step 4 If in use, remove the strain relief securing the power supply cable to the power supply latch.

Step 5 Remove the AC power cord from the power socket.

Step 6 Depress the power supply latch and use the handle to pull the supply out of the device.

Figure 28: Step 4

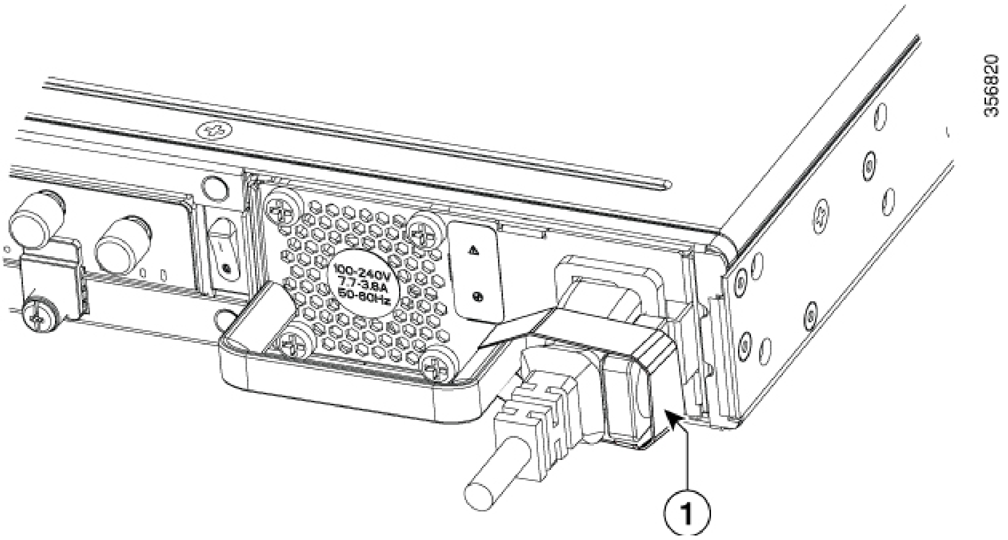


Figure 29: Step 5

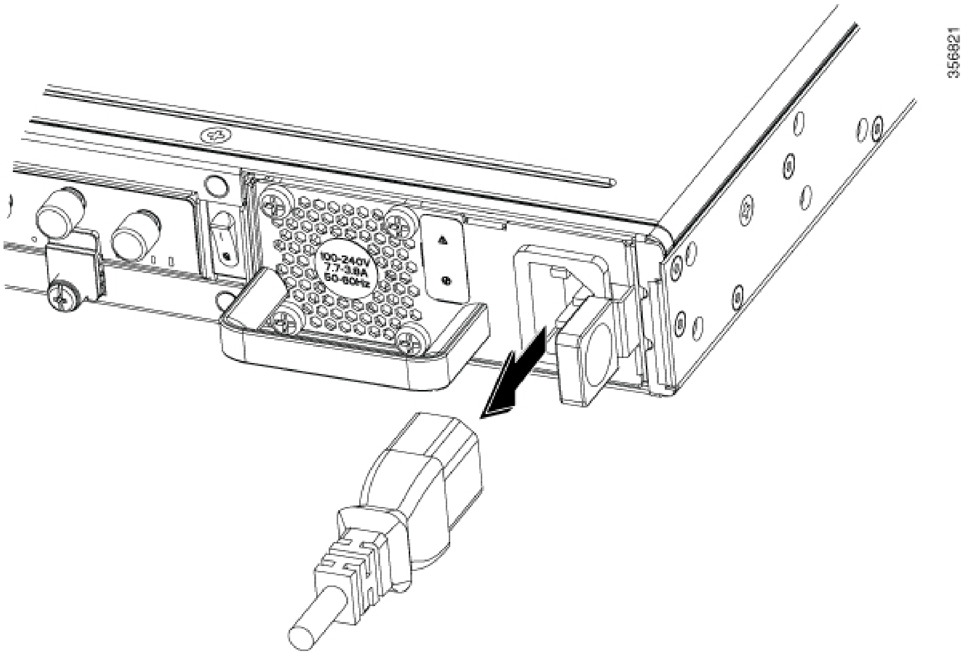
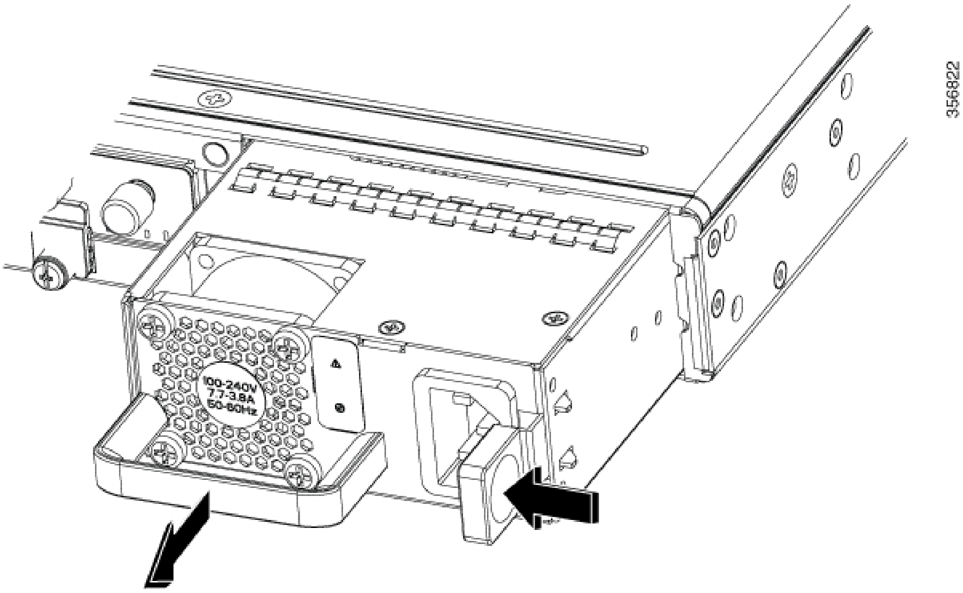


Figure 30: Step 6



To replace or install an AC power supply into the Cisco 8300 Series Secure Routers, perform these steps:

Procedure

Step 1 Use the handle to push the power supply into the router. The power supply latch should provide an audible click when the supply is fully seated.

Step 2 Install the AC power cord into the power socket on the power supply.

Step 3 If used, reapply the strain relief strap around the power cord and the power supply latch.

Step 4 If the device was turned off, turn the power back on to the device.

DC power supplies

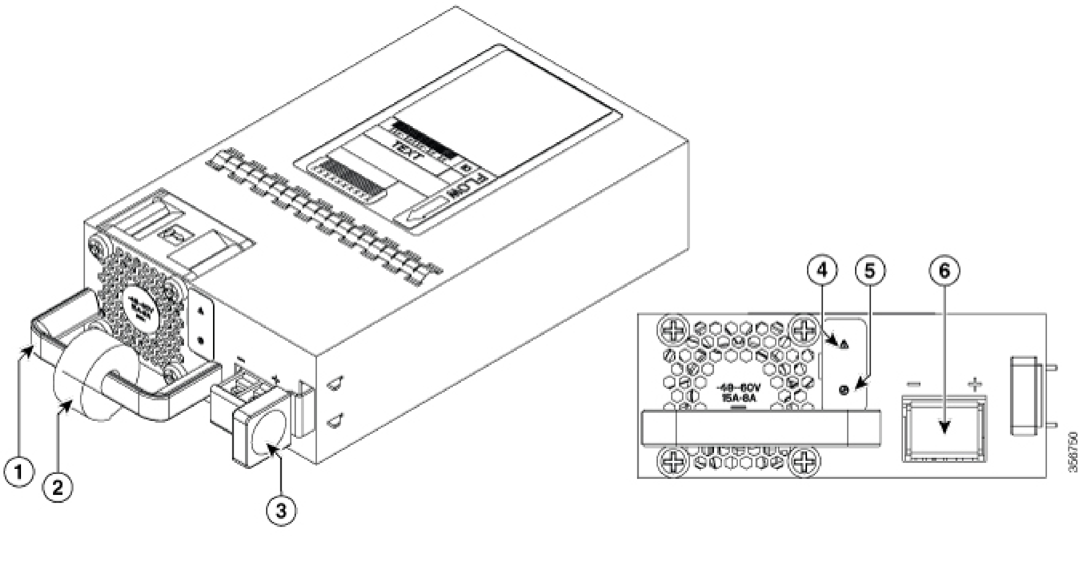
The Cisco 8300 Series Secure Routers have one DC power supply type. As with the AC power supplies, the DC power supplies are not of the same size and cannot be interchanged.

Overview of the DC power supplies

The DC power supply for Cisco 8300 Series Secure Routers devices is shown in the figure:

- PWR-CC1-500WDC

Figure 31: 500WDC power supply for C8375-E-G2



1	Handle	2	Strain relief
3	Latch	4	Fail LED
5	Status LED	6	Terminal block

Remove and Replace the DC Power Supply

To remove a DC power supply from a Cisco 8300 Series Secure Routers, perform these steps:

Procedure

Step 1 Read the safety warnings section of this document.

Step 2 If there is only one power supply in the system, shut down the device before removing the power supply.

Step 3 If there are redundant power supplies in use the device does not have to be shut down prior to replacing the power supply. The power supply may be replaced while the device is in service.

Step 4 At the power distribution panel or at the local circuit breaker, remove the power from the DC power leads (label **1**)attached to the power supply to be replaced.

Step 5 Remove the terminal block cover and loosen the terminal screws (label **1**) securing the power cabling. Remove the power cabling from the terminal block.

Step 6 Depress the power supply latch and use the handle to pull the supply out of the device.

Figure 32: Remove a DC Power Supply from the C8375-E-G2

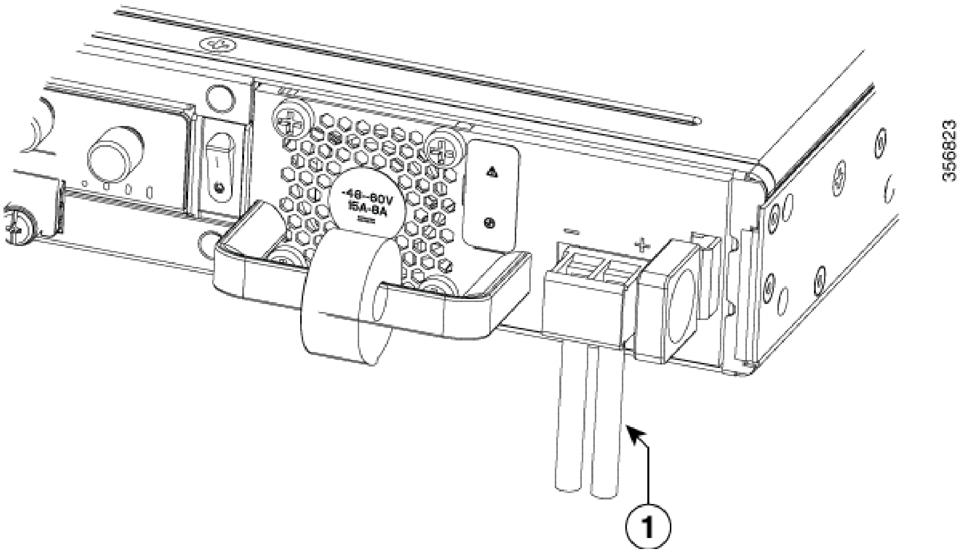


Figure 33: Step 5

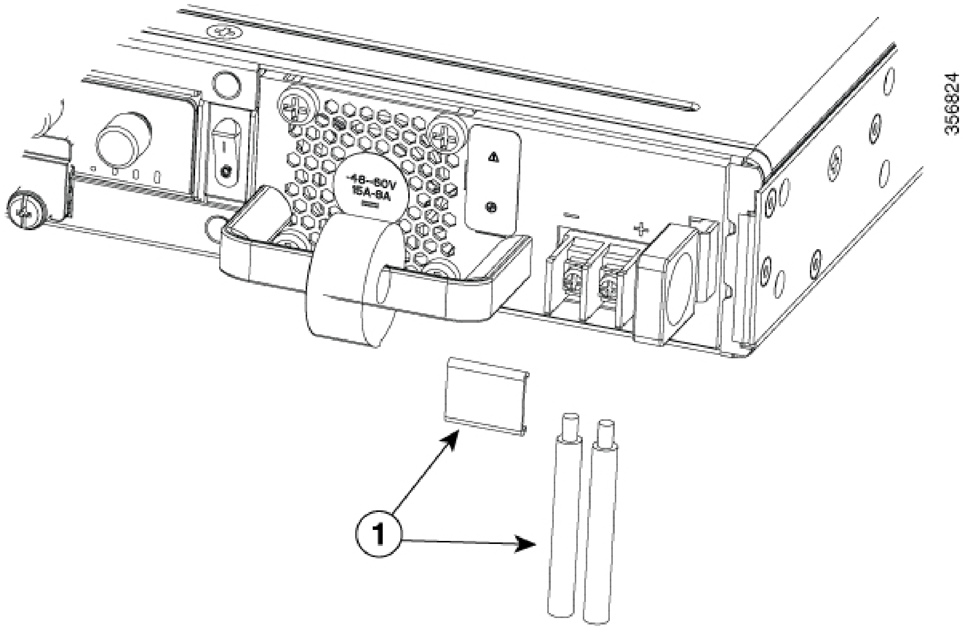
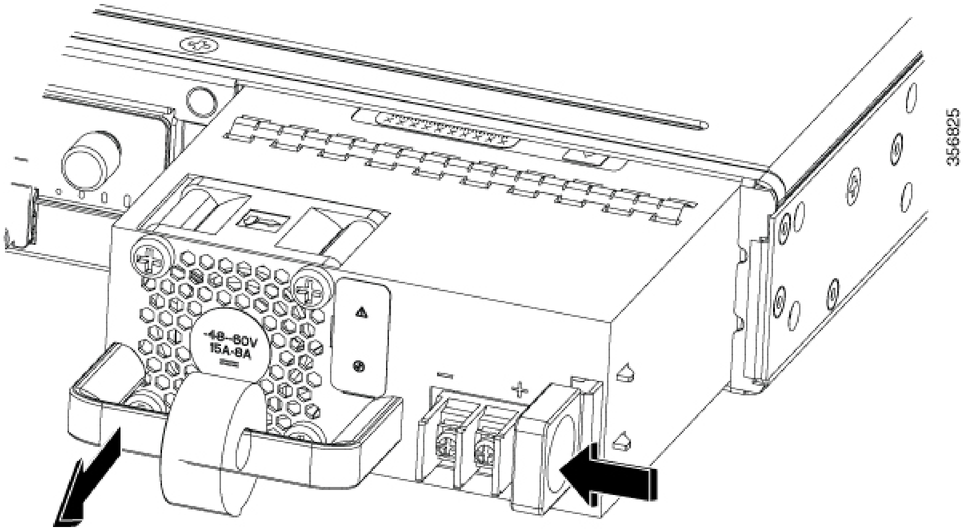


Figure 34: Step 6



To replace or install a DC power supply from a C8375-E-G2, perform these steps:

Procedure

Step 1 Use the handle to push the power supply into the router. The power supply latch should provide an audible click when the supply is fully seated.

Step 2 If this is an initial installation, please see the section on preparing the DC power leads below.

Step 3 Install the DC power leads into the terminal block and tighten the terminal block screws to secure the cables. For the PWR-CC1-400WDC power supply the negative lead installs into the left terminal position and the positive lead installs into the right terminal position. The polarity is marked on the faceplate of the power supply.

Caution
Do not over torque the terminal block captive screws. Ensure that the connection is snug, but the wire is not crushed. Verify by tugging lightly on each wire to ensure that they do not move.

Step 4 Reinstall the terminal block cover.

Step 5 If the device was turned off, turn the power back on to the device.

Install the DC input power

This section describes how to install the DC power supply input power leads to the Cisco 8300 Series Secure Routers DC input power supply. Before you begin, read these important notices:

- The color coding of the DC input power supply leads depends on the color coding of the DC power source at your site. Ensure that the lead color coding you choose for the DC input power supply matches the lead color coding used at the DC power source and verify that the power source is connected to the negative (–) terminal and to the positive (+) terminal on the power supply.
- Ensure that the chassis ground is connected on the chassis before you begin installing the DC power supply. Follow the steps provided in the Chassis Grounding .

Warning **Statement 1003—**DC Power Disconnection

To reduce risk of electric shock or personal injury, disconnect DC power before removing or replacing components or performing upgrades.

Prepare the wire for connecting to the DC power supply

In the Cisco 8300 Series Secure Routers, the DC power supply has a terminal block that is installed into the power supply terminal block header.

Use these steps to prepare the wire for connection to the terminal source:

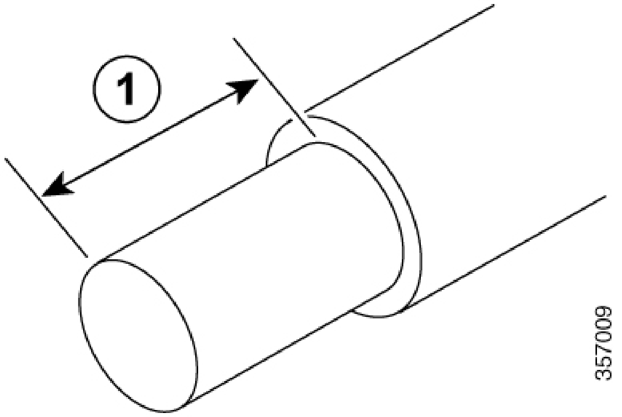
Procedure

Step 1 Turn off the circuit breaker from the power source to be connected to the power source. Ensure the wires to be attached to the power supply are not energized.

Step 2 The wires connecting to the power supply can be stripped back and terminated directly to the power supply terminal block. Alternately a crimp style spade terminal lug can be attached to the end of the wire. If using a terminal lug, follow the manufacturer's instructions for terminating the lug to the wire. If terminating directly to the terminal block using bare wire, following the directions shown below.

Use a wire-stripping tool to strip each of the two wires coming from the DC input power source to approximately 0.39 inch (10 mm) +/- 0.02 inch (0.5 mm). It is recommended that 14 AWG insulated wire be used. Do not strip more than the recommended length of wire because doing so could leave the wire exposed from the terminal block and shows a stripped DC input power source wire.

Figure 35: Stripped DC input power source wire



1	0.39 inch (10 mm) is the recommended wire-strip length for the terminal block.

Identify the positive and negative feed positions for the terminal block connection of C8375-E-G2:

a) Positive (+) lead wire (right)
b) Negative (–) lead wire (left)

Figure 36: DC power supply with lead wires

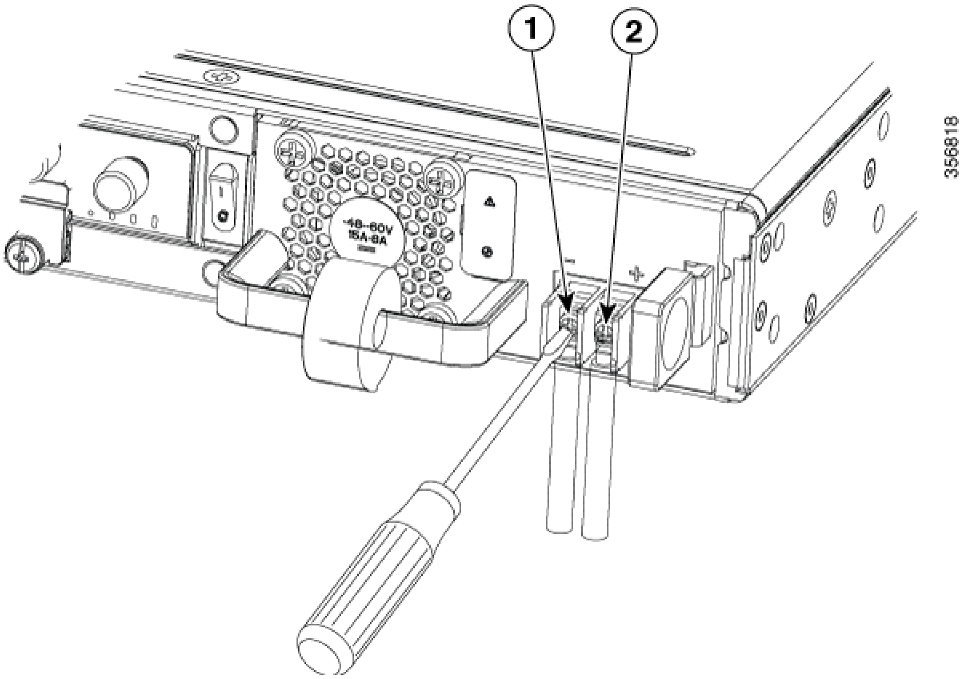


Table 9:

1	Negative (-) lead wire
2	Positive (+) lead wire

Replace a fan tray for Cisco 8300 Series Secure Routers

In the Cisco 8300 Series Secure Routers, we have fan trays that are field replaceable units (FRUs). The fan tray includes all the fans in one assembly. If a fan fails, replace the tray using a #1 Phillips screwdriver.

Before replacing a fan tray

Read the safety precautions below and have the required tools available before replacing a fan tray:

Remove the Fan Tray from a C8375-E-G2

The C8375-E-G2 supports forward air flow (standard version).

To replace the fan tray, perform these steps:

Procedure

Step 1 Power off the device

Step 2 Remove all cables from the chassis

Step 3 Remove unit from the equipment rack if it is installed in a rack

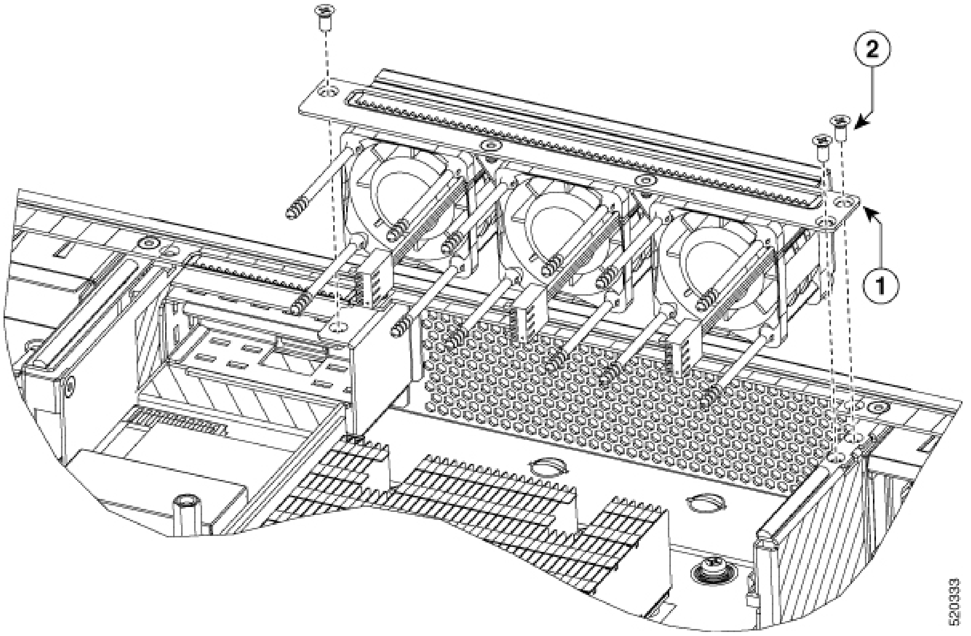
Step 4 Remove the top cover

Step 5 Remove the three screws from the fantray

Step 6 Disconnect fan cables from the motherboard

Step 7 Remove the fan tray

Note
The estimated time for replacing the fan tray on C8375-E-G2 by a skilled technician within 60 Minutes.



1	Fan tray	2	Screws

Install the Fan Tray into a C8375-E-G2

The C8375-E-G2 supports forward air flow (standard version).

To replace the fan tray, perform these steps:

Procedure

Step 1 Install the fan tray

Step 2 Install the three fan tray mounting screws

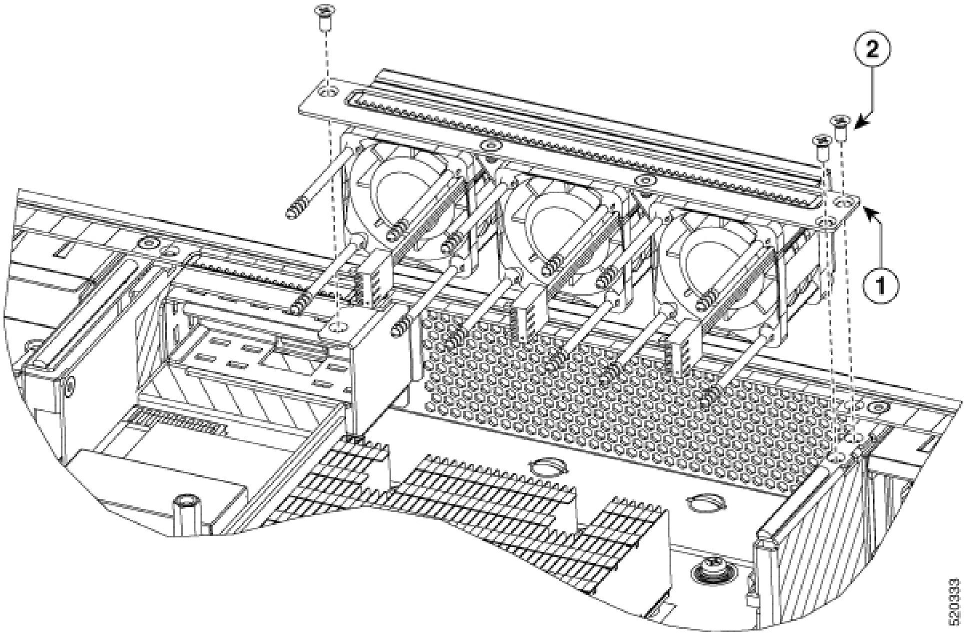
Step 3 Connect the fan cables to the motherboard

Step 4 Install the top cover

Step 5 If appropriate, re-install the unit back in an equipment rack

Step 6 Reinstall all cables from the chassis

Step 7 Power on the unit



1	Fan tray	2	Screws

Install and remove SFP and SFP+ Modules

Before you begin

See the Cisco 8300 Series Secure Routers' datasheet for a list of supported SFP and SFP+ modules. Use only supported SFP/SFP+ modules on the platform.

Warning **Statement 1008—**Class 1 Laser Product

This product is a Class 1 laser product.

Note We recommend that you wait 30 seconds between removal and insertion of an SFP on an interface module. This time is recommend to allow the transceiver software to initilize and synchronise with the standby RSP. Chaning an SFP more quickly could result in transceiver initialization issues that disable the SFP

- Do not remove the dust plugs from the SFP and SFP+ modules or the rubber caps from the fiber-optic cable until you are ready to connect the cable. The plugs and caps protect the module ports and cables from contamination and ambient light.

- Removing and installing an SFP and SFP+ module can shorten its useful life. Do not remove and insert any SFP/SFP+ module more often than is necessary.

- To prevent ESD damage, follow your normal board and component handling procedures when connecting cables to the switch and other devices.
- When you insert several SFP and SFP+ modules in multiple ports, wait for 5 seconds between inserting each SFP/SFP+. This will prevent the ports from going into error disabled mode. Similarly, when you remove an SFP and SFP+ from a port, wait for 5 seconds before reinserting it.

Procedure

Step 1 Attach an ESD-preventive wrist strap to your wrist and to an earth ground surface.

Step 2 Find the send (TX) and receive (RX) markings that identify the top of the SFP/SFP+ module.

On some SFP/SFP+ modules, the send and receive (TX and RX) markings might be shown by arrows that show the direction of the connection.

Step 3 If the SFP/SFP+ module has a bale-clasp latch, move it to the open, unlocked position.

Step 4 Align the module in front of the slot opening, and push until you feel the connector snap into place.

Step 5 If the module has a bale-clasp latch, close it to lock the SFP/SFP+ module in place.

Step 6 Remove the SFP and SFP+ dust plugs and save.

Step 7 Connect the SFP and SFP+ cables.

Laser safety guidelines

Optical Small-Form Pluggable (SFPs) use a small laser to generate the fiber-optic signal. Keep the optical transmit and receive ports covered whenever a cable is not connected to the port.

⚠ **Warning** **Statement 1051—**Laser Radiation

Invisible laser radiation may be emitted from disconnected fibers or connectors. Do not stare into beams or view directly with optical instruments.

⚠ **Warning** **Statement 1255—**Laser Compliance Statement

Pluggable optical modules comply with IEC 60825-1 Ed. 3 and 21 CFR 1040.10 and 1040.11 with or without exception for conformance with IEC 60825-1 Ed. 3 as described in Laser Notice No. 56, dated May 8, 2019.

To install an SFP module in your device, perform these steps:

Procedure

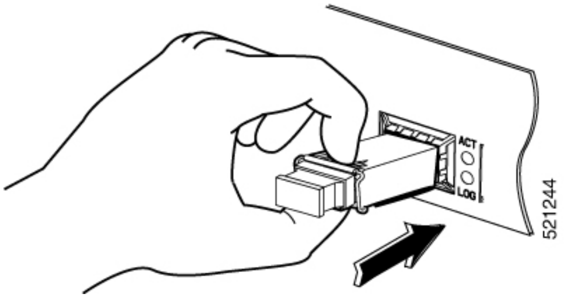
Step 1 Read the Safety Warnings and disconnect the power supply before you perform any module replacement.

Step 2 Slide the SFP into the device connector until it locks into position

Tip

If the SFP uses a bale-clasp latch (see Laser Safety Guidelines section, the handle should be on top of the SFP module.

Figure 37: Install a Small-Form Pluggable module



Caution

Do not remove the optical port plugs from the SFP until you are ready to connect cabling.

Step 3 Connect the network cable to the SFP module.

Remove Small Form Pluggable modules

Follow these steps to remove a Small Form Pluggable (SFP) from the device:

Procedure

Step 1 Read the Safety Warnings and disconnect the power supply before you perform any module replacement.

Step 2 Disconnect all cables from the SFP.

Warning

Statement 1051—Laser Radiation

Invisible laser radiation may be emitted from disconnected fibers or connectors. Do not stare into beams or view directly with optical instruments.

Caution

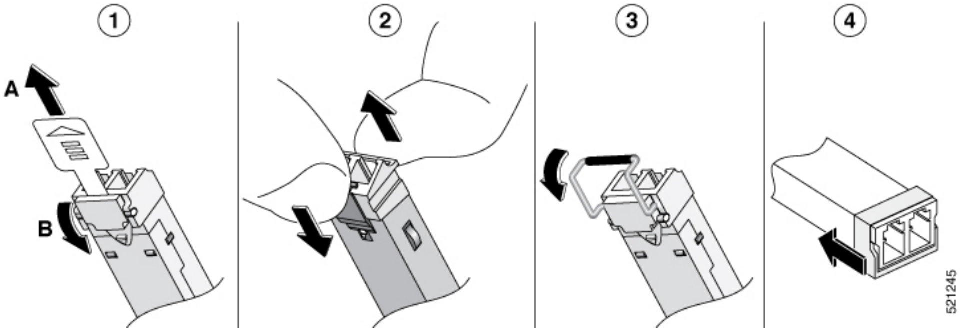
The latching mechanism used on many SFPs locks the SFP into place when cables are connected. Do not pull on the cabling in an attempt to remove the SFP.

Step 3 Disconnect the SFP latch.

Note

SFP modules use various latch designs to secure the module in the SFP port. Latch designs are not linked to SFP model or technology type. For information on the SFP technology type and model, see the label on the side of the SFP.

Figure 38: Disconnecting SFP latch mechanisms



1	Sliding latch	3	Bale-clasp latch
2	Swing and slide latch	4	Plastic collar latch

Tip

Use a pen, screwdriver, or other small straight tool to gently release a bale-clasp handle if you cannot reach it with your fingers.

Step 4 Grasp the SFP on both sides and remove it from the device.

Remove and replace the USB Flash Token memory stick

The Cisco 8300 Series Secure Routers contain ports for a USB memory stick to store Cisco configurations or Cisco IOS XE consolidated packages.

⚠ **Caution** Do not remove a USB Flash memory module when issuing some file access command or a read/write operation to the Flash memory module when it is processing. The router might reload or the USB Flash memory module can be damaged. You can check to see if the USB activity LED on the router front panel is flashing, prior to the removal of the USB device

To install, remove a USB memory stick from the device, perform these steps:

Procedure

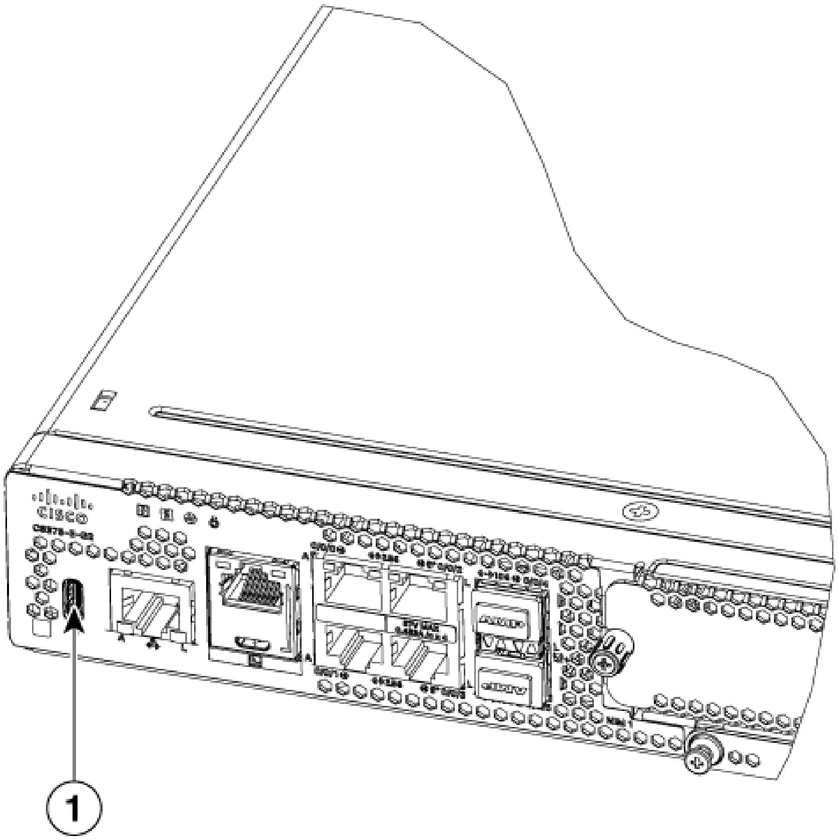
Step 1 Place the USB stick into the USB port.

Step 2 Type-C memory sticks are supported on USB port 1 and type-C memory can be inserted in any direction. Type-A memory sticks are supported on USB port 0 and it must be oriented correctly to allow for proper insertion.

Note

A sample of how the memory stick is inserted into the port.

Figure 39: USB memory stick



Note
You can insert or remove the memory stick whether the device is powered on or not.

1	USB Type C (3.0) (USB 0)

What to do next

This completes the USB Flash memory installation procedure.

Remove and install an M.2 USB|NVMe module

This section describes installing and replacing an M.2 USB|NVMe module on the Cisco 8300 Series Secure Routers.

Prevent electrostatic discharge damage

The M.2 module is sensitive to electrostatic discharge (ESD) damage, which can occur when electronic cards or components are handled improperly. ESD results in complete or intermittent failures.

To prevent ESD damage, follow these guidelines:

- Always use an ESD wrist or ankle strap and ensure that it makes good skin contact.
- Connect the equipment end of the strap to an unfinished chassis surface.
- Place the M.2 storage devices on an anti-static surface or in a static shielding bag. If you have to return the device to the factory, immediately place it in a static shielding bag.
- Avoid contact between the device and clothing. The wrist strap protects the device from ESD voltages on the body only; ESD voltages on clothing can still cause damage.
- Do not remove the wrist strap until the installation is complete.

⚠

Caution For safety, periodically check the resistance value of the anti static strap. The measurement should be between 1 and 10 megohms (Mohms).

Remove the M.2 USB|NVMe module

To remove a M.2 USB|NVMe module, perform these steps:

Note The M.2 USB|NVMe module installation for C875-E-G2. The M.2 USB|NVMe modules are flipped upside down.

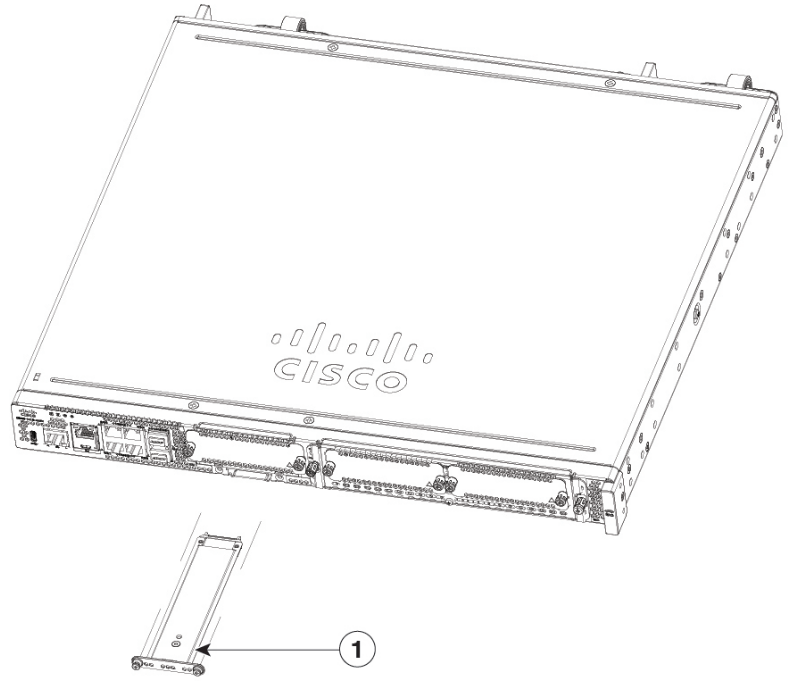
Procedure

Step 1 The device should be powered down and the power supply disconnected before you perform any module replacement.

Step 2 Loosen 2 mounting screws using a #1 Philips screwdriver.

Step 3 Gently pull the M.2 USB|NVMe module out and remove it from the device.

Figure 40: Remove the M.2 USB|NVMe module (C8375-E-G2)



1	M.2 USB|NVMe module

Install the M.2 USB|NVMe module

To install the M.2 USB|NVMe module, perform these steps:

Note For the C8375-E-G2, the PCB faces down.

Procedure

Step 1 Read all Safety Warnings, ensure that the C8375-E-G2 is not powered on.

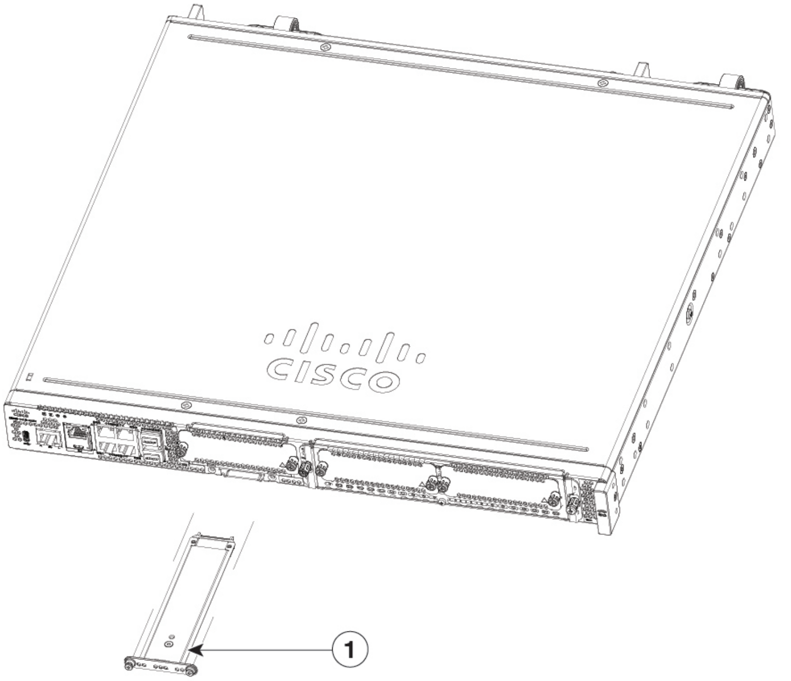
Step 2 Insert the M.2 USB|NVMe module into the slot of the device (as shown in the figure). The slide should engage the internal card guides.

Step 3 Gently slide the M.2 USB|NVMe module all the way in until the faceplate is flush with the device.

Step 4 Screw down and tighten the two Philips head screws. Torque it to 4-6 in lbs.

Step 5 The device can now be powered on.

Figure 41: Install the M.2 USB|NVMe (C8375-E-G2)



1	M.2 USB|NVMe

Managing self encrypting drives

Cisco 8300 Series Secure Routers support self-encrypting drives (SED), which helps to enhance the security of data that are stored on these platforms. SEDs are locked using a security key. The security key, which is also known as Key-Encryption Key or an authentication passphrase is used to encrypt the media encryption key. If the disk is not locked, no key is required to retrieve the data. To enable the security lock, use the **hw-module harddisk security-lock enable to enable the** command. To disable the security lock, use **the no hw-module harddisk security-lock enable** command.

Also, you can perform these actions:

- To check the security status, use the **show hw-module harddisk security-lock status** command.
- To perform factory reset on the SED when the security-lock is enabled, use the **factory-reset sed**
- To perform factory reset on the SED without checkig the status of the security-lock, use the **factory-reset sed PSID** command. The PSID (Physical Secure ID) is a 32 character ASCII string read from the label attached to the SED drive.

CHAPTER 5

Install Cisco Catalyst Network Interface Module

This section provides information before and during the installation of Cisco Catalyst Network Interface Modules (NIMs) on the Cisco 8300 Series Secure Routers.

Overview of the Network Interface Module

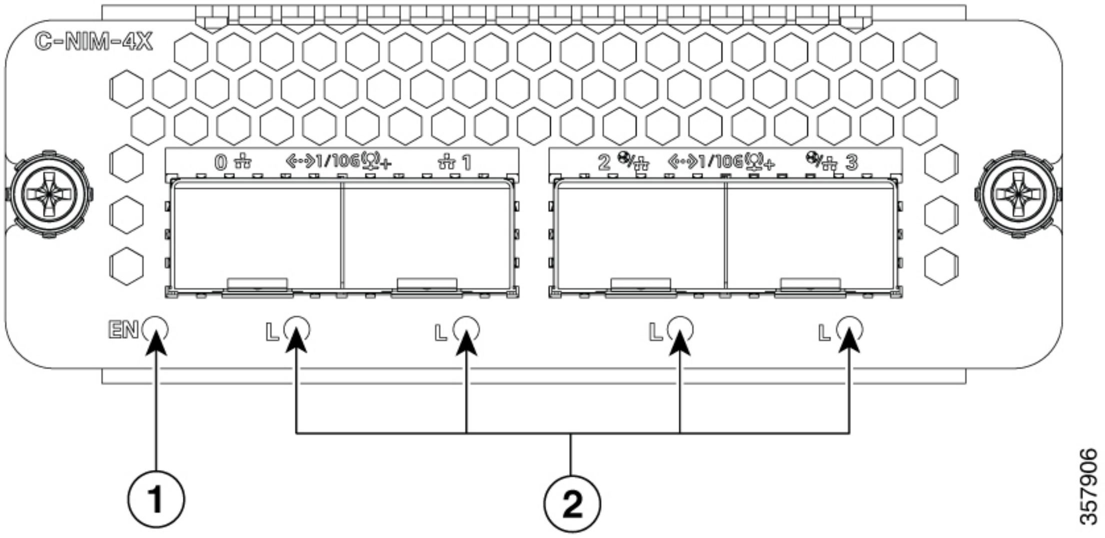
The Cisco Catalyst Network Interface Module (NIM), which has 10G WAN and 4xSFP+ 10G port is supported on Cisco 8300 Series Secure Routers.

For additional information, see the Cisco 8300 Series Secure Routers datasheet on cisco.com for a list of supported NIMs on the platforms.

Front panel of Catalyst NIM

Figure shows the front panel of the Catalyst Network Interface Module:

Figure 42: Front panel of catalyst NIM



	LED	Color	Description
1	LED EN (Enable)	Green/Amber	Off: Power off Solid Green: Power on and operate normally Solid Amber: Power or operataing failure
2	SFP Ports L (Link)	Green/Amber	Off: No link. SFP is not detected or inserted Solid Green: SFP link up Solid Amber: SFP is not supported or in a fault state

Remove and install Network Interface Modules

Keep these tools and equipment while working with the Network Interface Modules (NIM)s:

- Number 1 Phillips screwdriver or a small flat-blade screwdriver
- ESD-preventive wrist strap

Remove the Network Interface Module

Step 1 Shut down the electrical power to the slot in the device, turn off the electrical power to the device. Leave the power cable plugged-in to channel ESD voltages to ground.

Step 2 Remove all network cables from the rear panel of the device. Using a number 1 Phillips screwdriver, loosen the captive screws on the network interface module.

Step 3 Slide the network interface module out.

Step 4 If you are not replacing the module, install a blank faceplate over the empty slot to ensure proper air flow.

Install the Cisco Catalyst Network Interface Modules

Step 1 Shut down the electrical power to the slot in the router by turning off the electrical power to the router. Leave the power cable plugged in to channel ESD voltages to ground.

Step 2 Remove all network cables from the rear panel of the device.

Step 3 Remove the blank faceplates installed over the network interface module slot that you intend to use.

Note Save blank faceplates for future use.

Step 4 Align the module with the guides in the chassis walls or slot divider and slide it gently into the NIM slot on the device.

Step 5 Push the module into place until you feel the edge connector seat securely into the connector on the router backplane. The module faceplate should contact the chassis rear panel.

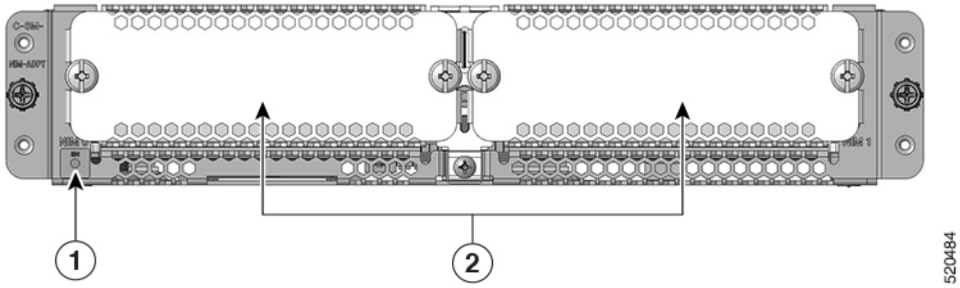
Step 6 Using a number 1 Phillips screwdriver, tighten the captive screws on the network interface module.

Step 7 Connect the module to the network and re-enable the power to the slot in the device.

Remove and install Network Interface Modules adapter

This section provides information for before and during the installation of the Cisco Catalyst NIM adapter for two Cisco network interface modules (NIMs) on the Cisco 8300 Series Secure Routers.

Figure 43: Front panel of Cisco Catalyst NIM adapter



	Description
1	**LED: EN** Off: Device power is off, or the adapter has not yet started. (It may take several seconds for the adapter to start after the router is powered on.) Green, solid: Powered on and functioning normally. Amber, solid: Module has some type of failure.
2	NIM slots

Remove the Network Interface Module Adapter

Before You Begin

- Read the safety warnings section before beginning this procedure.
- The Cisco Catalyst NIM adapter is considered "hot swappable." Removing the adapter does not require powering off the device.
- When preparing to remove the Cisco Catalyst NIM adapter, first remove any installed NIMs, and then remove the adapter.

Procedure

To remove the Cisco Catalyst NIM adapter from a service module (SM) slot on a Cisco 8300 Series Secure Routers:

Step 1 Locate the NIM adapter to be removed. Using a number 1 Phillips or flat-blade screwdriver, unscrew the captive mounting screws on the module faceplate.

Step 2 Pull the NIM adapter out of the chassis.

Step 3 Align the module with the guides in the chassis walls or slot divider and slide it gently into the NIM slot on the device.

Step 4 Place the NIM adapter in an antistatic bag to protect it from electrostatic discharge (ESD) damage.

Step 5 Install a blank faceplate over the empty slot to ensure proper air flow.

Install Network Interface Module adapter

Before You Begin

- Read the safety warnings section before beginning this procedure.
- The Cisco Catalyst NIM adapter is considered 'hot swappable'. Installing the adapter does not require powering off the device.
- Do not install network interface modules (NIMs) into the Cisco Catalyst NIM adapter before installing the adapter in the chassis.

- When preparing to remove the Cisco Catalyst NIM adapter, first remove any installed NIMs, then remove the adapter.

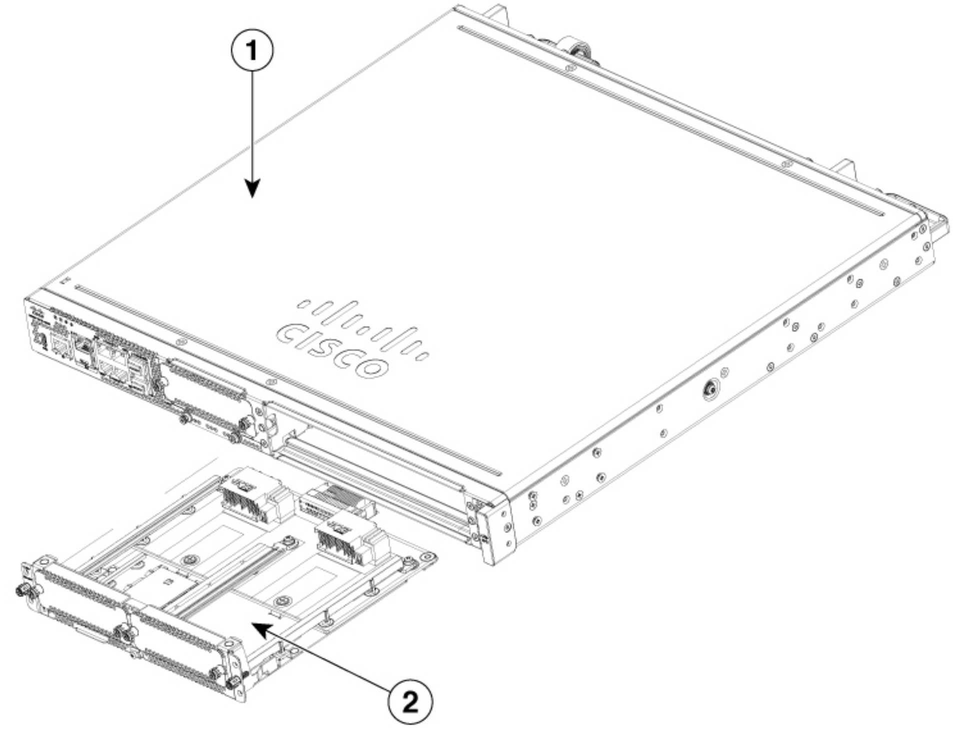
Procedure

To install the Cisco Catalyst NIM adapter into a service module (SM) slot on a Cisco 8300 Series Secure Routers:

1. Remove the blank faceplate installed over one of the device SM slots. The position of the slots depends on the platform's form factor: 1 rack unit (RU) or 2 RU, as shown below.

Note Save blank faceplates for future use.

Figure 44: Cisco Catalyst SM-NIM Adapter on C8375-E-G2



	Description
1	Chassis
2	Cisco C-SM-NIM adapter

2. Align the Catalyst NIM adapter with the guides in the chassis walls or slot divider and slide it gently into a service module (SM) slot on the router.

3. Push the Catalyst NIM adapter into place until you feel the edge connector seat securely into the connector on the router backplane. The faceplate should contact the chassis rear panel.

4. Using a number 1 Phillips screwdriver, tighten the captive screws on the network interface module.
5. Check the LED on the Catalyst NIM adapter and confirm proper operation.

Note A solid green LED indicates that the Catalyst NIM adapter is correctly inserted. It may take several seconds for the adapter to start before the LED is solid green.

6. (Optional) Install either one or two network interface modules into the Catalyst NIM adapter after it has been installed in the chassis. Follow the instructions for installing the NIM.

Install Network Interface Modules in the NIM adapter

The Cisco Catalyst NIM adapter provides two network interface module (NIM) slots. To install a NIM into the adapter, follow the instructions for the NIM.

Note

- Install the Cisco Catalyst NIM adapter into the router chassis before installing any NIMs into the adapter.
- Before removing the Cisco Catalyst NIM adapter from the chassis, first remove any NIMs that have been installed into the adapter.

CHAPTER 6

Install Cisco Catalyst Service Module

This section describes how to install the Cisco Catalyst Service Modules on the Cisco 8300 Series Secure Routers. The service modules supported on the on the Cisco 8300 Series Secure Routers are:

- C-SM-16P4M2X

For additional information on the supported SMs, see the Cisco 8300 Series Secure Routers' datasheet on cisco.com.

Note

- Only one service module is supported within a single chassis at a time
- Reload the system when you need to switch between the switching modes
- You can perform online insertion and removal of the modules. After installing the service module, you must reload the system to enable and activate the next-generation switching feature set.

Prepare for installation

This section describes safety warnings, general maintenance guidelines, and safety recommendations that you must read before installing and using the service module:

Equipment that you need

- Ratcheting torque screwdriver with a number-2 Phillips head that exerts a maximum of 15 pound-force inches (lbf-in.) of pressure
- Wire-stripping tools
- 12-gauge copper ground wire (insulated or not) for the single-hole ground connection

- Single-hole ground lug and screw (included in the accessory kit)
- Four leads of 14-gauge copper wire

Remove the Cisco Catalyst Service Module

Perform these steps to remove the service modules from the chassis:

Procedure

Step 1 Read the Safety Warnings before you perform any module replacement.

Step 2 Locate the service module(s) to be removed

Step 3 Unscrew the captive mounting screws on the module faceplate using a number 1 Phillips or flat-blade screwdriver.

Step 4 Pull the module out of the chassis.

Step 5 For the module, keep the latches in open position and pull the module out of the chassis.

Step 6 Place the service module in an antistatic bag to protect it from electrostatic discharge (ESD) damage.

Install a Cisco Catalyst Service Module

This section describes how to install the service modules.

Note For illustration purposes, we have used image of Cisco C-SM-X-16P4M2X.

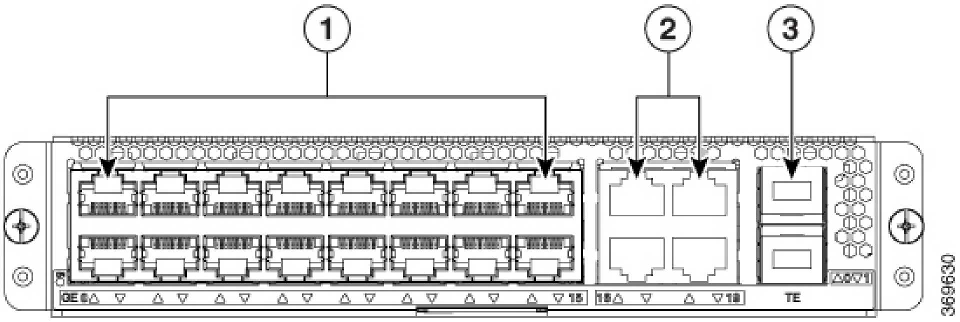
After the device boots up, insert the C-SM-X-16P4M2X module into the slot of the chassis. A system message displays: : *Jun 10 13:58:14.367 CST: %IOMD-3-UNSUPPORTED_NGSWITCH: R0/0: iomd:*

The message denotes that the system is in legacy switching mode. For the legacy switching mode to take effect, you need to reload the slot 1 bay 0 of the switch module for the SM-X-16P4M2X service module. Also, you need to reload the device to get the module working.

Caution Always wear an electrostatic discharge (ESD)-preventive wrist strap and ensure that it makes good contact with your skin when you install or remove the C-SM-X-16P4M2X service module. Connect the equipment end of the wrist strap to the metal part of the chassis.

Caution Handle your service modules only by their edges. Service modules are ESD-sensitive components and can be damaged by mishandling.

Figure 45: Front panel of the single-wide Service Module



1	GE copper port	3	1G/10G SFP/SFP+ port
2	2.5G mGiG copper port		

To install a service module on your device, perform these steps:

Procedure

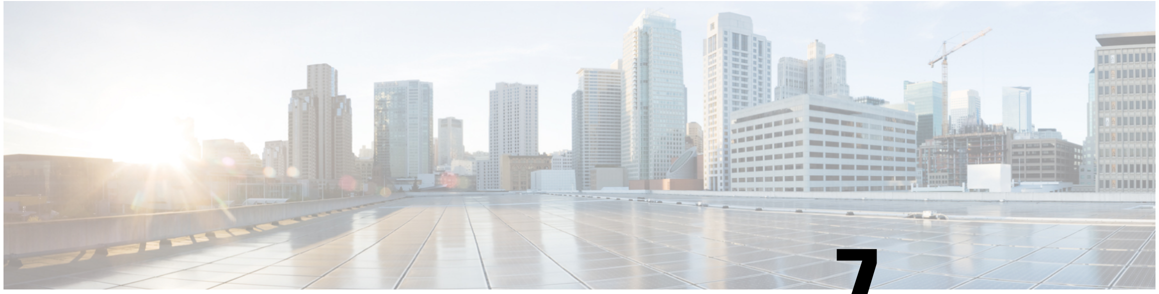
Step 1 Read the Safety Warnings before you perform any module replacement.

Step 2 For the module, remove the blank faceplate installed over the slot you intend to use.

Step 3 For the module, remove both the blank faceplates and the divider installed over the slot you intend to use.

Step 4 With the service module, push the module into place until you feel the edge connector seat securely into the connector on the backplane. The module faceplate should contact to the chassis panel.

Step 5 Using a number 1 Phillips or flat-blade screwdriver, tighten the captive mounting screws on the module faceplate.



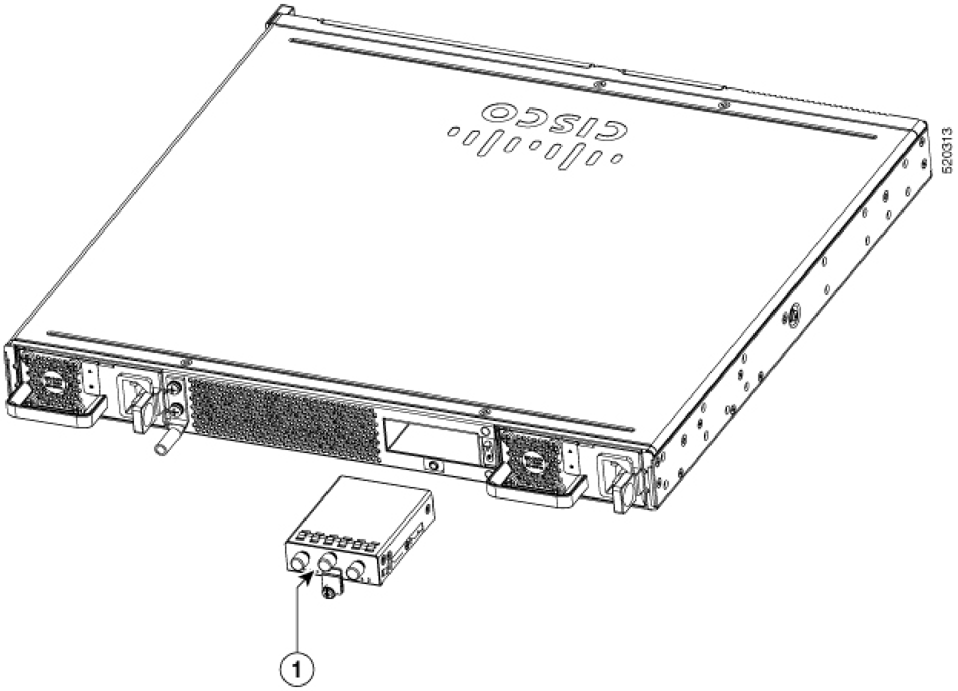
CHAPTER 7

Cisco Catalyst Pluggable Interface Module

This section provides information before and during the installation of Cisco Catalyst Pluggable Interface Module (PIM) on the Cisco 8300 Series Secure Routers.

For additional information on the supported NIMs, see the Cisco 8300 Series Secure Routers' datasheet on cisco.com for a list of supported PIMs on the platforms.

Figure 46: Pluggable Interface Module in a C8375-E-G2



1	Pluggable interface module

Safety recommendations

To prevent hazardous conditions, follow these safety recommendations while working with this equipment:

- Keep tools away from walk areas where you or others could fall over them.
- Do not wear loose clothing around the router. Fasten your tie or scarf and roll up your sleeves to prevent clothing from being caught in the chassis.
- Wear safety glasses when working under any conditions that might be hazardous to your eyes.
- Locate the emergency power-off switch in the room before you start working. If an electrical accident occurs, shut the power off.
- Before working on the router, turn off the power and unplug the power cord.
- Disconnect all power sources before doing the following:
    - Installing or removing a router chassis
    - Working near power supplies
- Do not work alone if potentially hazardous conditions exist.
- Always check that power is disconnected from a circuit.
- Remove possible hazards from your work area, such as damp floors, ungrounded power extension cables, or missing safety grounds.
- If an electrical accident occurs, proceed as follows:
    - Use caution; do not become a victim yourself.
    - Turn off power to the room using the emergency power-off switch.
    - Determine the condition of the victim and send another person to get medical aid or call for help.
    - Determine if the person needs rescue breathing or external cardiac compressions; then take appropriate action.

Tools and equipment required during installation

You will need the following tools and equipment while working with the Cisco C-NIM-1X NIM:

- Number 1 Phillips screwdriver or a small flat-blade screwdriver
- ESD-preventive wrist strap

Remove Cisco Catalyst Pluggable Interface Module

To remove a PIM, perform these steps:

Procedure

Step 1 Read the Safety Warnings before you perform any task.

Step 2 Power down the unit and remove power from the power supplies.

Step 3 Loosen the Phillips head screw on the module faceplate, and then pull out the module by gripping the screw.

Install a Cisco Catalyst Pluggable Interface Module

To install a PIM, perform these steps:

Procedure

Step 1 Read the Safety Warnings before you perform any task.

Step 2 Power down the unit and remove power from the power supplies.

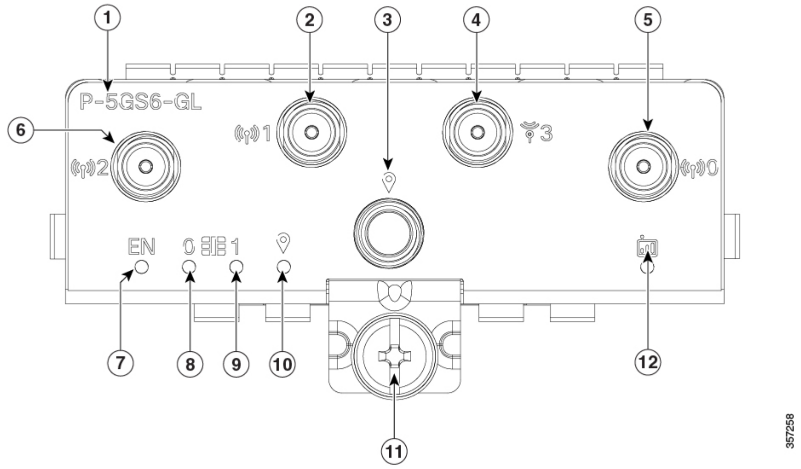
Step 3 If there is a filler faceplate blank in the PIM slot, loosen the Phillips head screw and remove the blank.

Step 4 Push the module into the slot until you feel the edge connector seat into the connector on the backplane. The module faceplate should contact the chassis panel.

Step 5 Tighten the Phillips head screw on the module faceplate.

Step 6 The device may now be powered on.

Figure 47: 5G Pluggable Interface Module - P-5GS6-GL

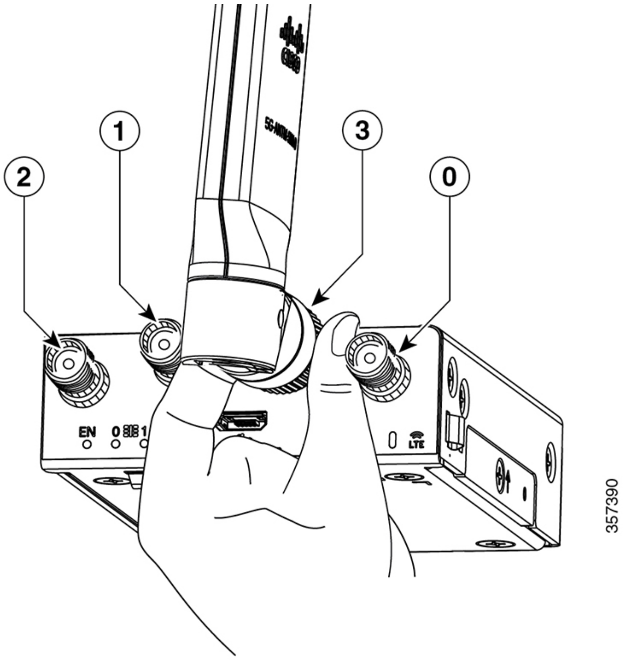


1	PID
2	Antenna 1 (SMA)
3	GPS (SMA)
4	Antenna 3 (SMA, reception only)
5	Antenna 0 (SMA)
6	Antenna 2 (SMA)
7	Enable LED
8	SIM 0 LED
9	SIM 1 LED
10	GPS LED
11	M3.5 thumb-screw
12	Service LED

Configuring a Pluggable Interface Module

To insert the antenna in the Pluggable Interface Module, perform the below steps:

Figure 48: Attaching the antennas



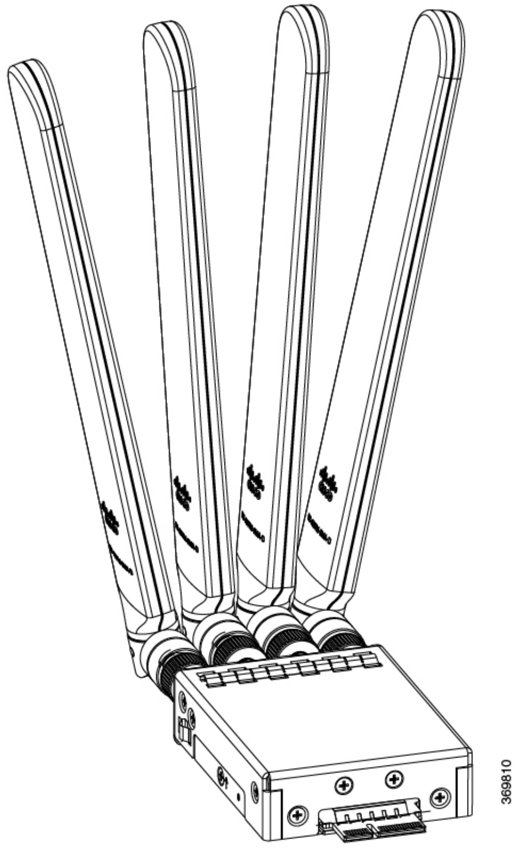
Procedure

Step 1 Use your thumb and index finger to insert and tighten antenna 1 and antenna 3 in the middle antenna attachment slots as indicated in the figure.

Note
While installing the antennas, first install antenna 1 and antenna 3 (this instruction is for the two antenna attachments present in the middle) and secure it completely. If you install antenna 2 and antenna 0 first (this refers to the first and the last antenna attachments), there will be less space to insert your thumb and index finger and therefore you may not be able to secure antenna 1 and 3.

Step 2 Insert antenna 2 and antenna 0 in the first and last antenna attachment slots.

Step 3 After installing the antennas, adjust the antenna orientation by spacing out each of them equally until they are spread out. This is important as it helps in getting higher RF performance.



RF Band Mapping for antenna ports (For P-5GS6-GL only)

The following table lists the RF band mapping for antenna ports.

RF Band mapping for antenna ports:

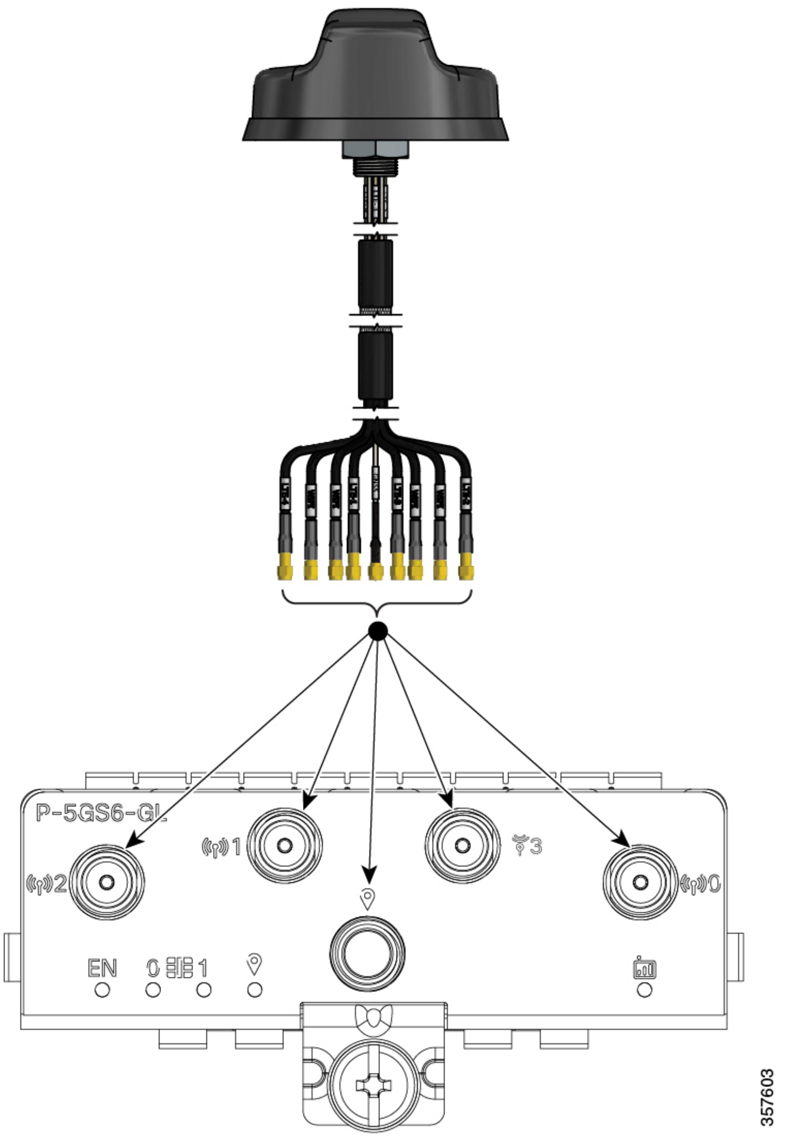
Antenna Port	Technology	TX	RX
ANT 0	3G WDCMA	B1, B2, B3, B4, B5, B6, B8, B9, B19	B1, B2, B3, B4, B5, B6, B8, B9, B19
	LTE	B1, B2, B3, B4, B5, B7, B8, B12, B13, B14, B17, B18, B19, B20, B25, B26, B28, B30, B34, B38, B39, B40, B41, B66, B71	B1, B2, B3, B4, B5, B7, B8, B12, B13, B14, B17, B18, B19, B20, B25, B26, B28, B29, B30, B32, B34, B38, B39, B40, B41, B42, B43, B46, B48, B66, B71
	5G NR FR1	n1, n2, n3, n5, n7, n8, n12, n20, n28, n38, n40, n41, n66, n71	n1, n2, n3, n5, n7, n8, n12, n20, n25, n28, n38, n40, n41, n48, n66, n71, n77, n78, n79

Antenna Port	Technology	TX	RX
ANT 1	3G WDCMA	-	B1, B2, B3, B4, B5, B6, B8, B9, B19
	LTE	B5, B20, B42, B43, B48, B71	B1, B2, B3, B4, B5, B7, B8, B12, B13, B14, B17, B18, B19, B20, B25, B26, B28, B29, B30, B32, B34, B38, B39, B40, B41, B42, B43, B46, B48, B66, B71
	5G NR FR1	n5, n48, n77, n78, n79	n1, n2, n3, n5, n7, n8, n12, n20, n25, n28, n38, n40, n41, n48, n66, n71, n77, n78, n79
ANT 2	3G WDCMA	-	-
	LTE	B1, B2, B3, B4, B7, B41, B66	B1, B2, B3, B4, B7, B25, B30, B32, B34, B38, B39, B40, B41, B42, B43, B46, B48, B66
	5G NR FR1	n1, n2, n3, n7, n25, n41, n66, n77, n78, n79	n1, n2, n3, n7, n25, n38, n40, n41, n48, n66, n77, n78, n79
ANT 3	3G WDCMA	-	-
	LTE	-	B1, B2, B3, B4, B7, B25, B30, B32, B34, B38, B39, B40, B41, B42, B43, B46, B48, B66
	5G NR FR1	-	n1, n2, n3, n7, n25, n38, n40, n41, n48, n66, n77, n78, n79

Attaching the antennas

To attach the antenna in the Pluggable Interface Module, perform the below steps:

Figure 49: Attaching 5G NR Antenna (5G-ANTM-O4-B) to P-5GS6-GL PIM



Note 5G NR Antenna (5G-ANTM-04-B) is supported on both P-LTEAP18-GL and P-5GS6-GL PIMs.

1. Attach each SMA cable to the ports as indicated in the table mappings.
2. Ensure that you tighten and secure each SMA cable into the SMA connector on the PIM.

Table 10: Port Mappings for 5G-ANTM-0-4-B on P-5GS6-GL and P-LTEAP18-GL PIMs

5G-ANTM-O-4-B	P-LTEAP18-GL	P-5GS6-GL
MAIN 0 (LTE1)	Main 0	ANT 0
MAIN 1 (LTE3)	Main 1	ANT 1
DIV 0 (LTE2)	DIV 0	ANT 2
DIV 1 (LTE4)	DIV 1	ANT 3
GNSS	No connection	GPS

This link contains the antenna specifications and installation instructions for 5G NR (5G-ANTM-O-4-B):

https://www.cisco.com/c/en/us/td/docs/routers/connectedgrid/antennas/installing-combined/b-cisco-industrial-routers-and-industrial-wireless-access-points-antenna-guide/m-5g-antm-04b.html#Cisco_Generic_Topic.dita_e780a6fe-fa46-4a00-bd9d-1c6a98b7bcb9

CHAPTER 8

Online Insertion and Removal and Hot-Swapping

The online insertion and removal (OIR) operation lets you replace faulty data and voice modules without affecting system operations. The OIR is similar to hot-swapping. OIR commands are issued before removing and after installing a module. When performing OIR, use an identical module to replace an original one. If you need to perform the OIR operation on multiple modules within a router, perform the operation one module at a time.

The difference between hot-swapping and OIR is that OIR requires executing Cisco IOS commands before and after the OIR. Hot-swapping is strictly a hardware function and does not require the execution commands. Not all router components or modules use OIR, or can be hot swapped.

The following components use OIR in the routers:

- Service Modules (SMs)
- Network Interface Modules (NIMs)
- SFPs
- USB devices

The following components can be hot swapped:

- Power supply: only when the router is backed up with an optional PSU

Requirement

To issue OIR commands, you must keep the module that is to be replaced in EnergyWise full-power mode. If the module is in EnergyWise power-saving or shutdown mode, you cannot issue OIR commands, and you cannot, therefore, remove the module.

OIR procedures

The following procedures describe using the OIR process to remove and replace NIMs and SMs.

Remove a module

From a console terminal run the **hw-module subslot subslot stop** command. The service module adapter LED blinks, turns off, and the console displays a prompt signaling the module can be removed. See the output:

```
Device# hw-module subslot 2/0 stop
Proceed with stop of module? [confirm]
damo-O2#
*Mar 22 20:43:31.088: %SPA_OIR-6-OFFLINECARD: SPA (SM-X-1T3/E3) offline in subslot 2/0
*Mar 22 20:43:31.088: %IOSXE_OIR-6-SOFT_STOPSPA: SPA(SM-X-1T3/E3) stopped in subslot 2/0,
interfaces disabled
Device# show hw-module subslot 2/0 oir
Module Model Operational Status
------------- -------------------- ------------------------
subslot 2/0 SM-X-1T3/E3 stopped
```

Insert a module

You require to run this step only if you run the oir-stop command when the module is not physically removed from the slot. If the module is physically removed, you do not require to run this command.

From a console terminal issue the hw-module sm {slot} oir-start command. The console displays output that shows the module change states:

```
Device# hw-module sm 2 oir-start
Device#
*Nov 11 21:06:17.546: %ATMOC3POM-6-SFP_IN: Interface ATM2/0 OC3 MM SFP has been inserted.
Router#
*Nov 11 21:06:19.442: %LINK-3-UPDOWN: Interface ATM2/0, changed state to up
*Nov 11 21:06:20.442: %LINEPROTO-5-UPDOWN: Line protocol on Interface ATM2/0, changed state
 to up
```