Hardware Installation Guide for the Cisco 8200 Series Secure Routers

First Published: 2025-09-10

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.

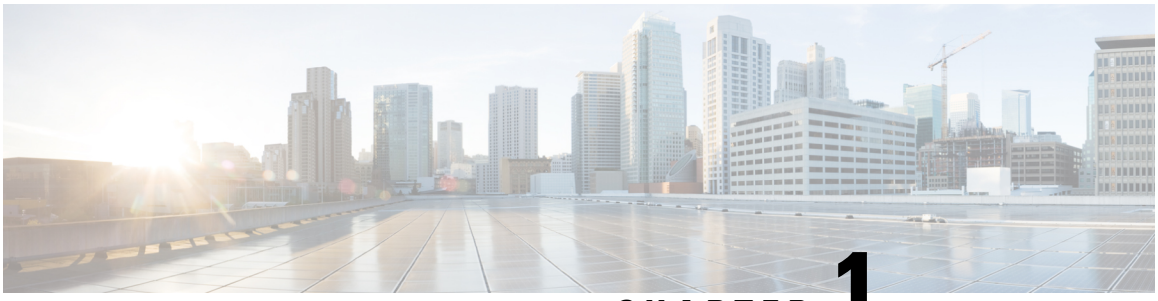
Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual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

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: https://www.cisco.com/c/en/us/about/legal/trademarks.html. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1721R)

CONTENTS



CHAPTER 1

Overview of Cisco 8200 Series Secure Routers

Cisco 8200 Series Secure Routers deliver secure networking simplified. Powered by the all-new secure networking processor and the unified Cisco secure networking platform, Cisco 8200 Series Secure Routers deliver robust, platform-level security, advanced performance engineering via 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.

About Cisco 8200 Series Secure Routers

Designed for medium branch deployments, Cisco 8200 Series Secure Routers combine robust security, advanced performance engineering, and flexible management options. These routers offer seamless connectivity, dynamic path selection, and unified security enforcement, ensuring resilient operations and simplified IT overhead as your network grows. With integrated security and support for high-speed 10G interfaces, these platforms deliver scalable and reliable performance for modern WAN edge deployments.

Table 1: Base Models of the Cisco 8200 Series Secure Routers

Base Models	Front Panel Switch Ports	Management Ports	WAN Ports	Console Port	(Optional) POE	(Optional) WLAN	USB Type C
C8231-G2	8	1 RJ-45	2 SFP +	Serial RJ-45	PoE Output -53.5VDC (port 7), 0.56A, 30 W max	None	5V, 1.5A max

Base Models	Front Panel Switch Ports	Management Ports	WAN Ports	Console Port	(Optional) POE	(Optional) WLAN	USB Type C
C8235-G2	8	1 RJ-45	2 SFP +	Serial RJ-45, Micro USB	PoE output -54VDC, 555mA (Port 4-5) and 1.66A (Port 6-7) total 120W max	None	5V, 1.5A max

Note C8231-G2 has 8GB of DRAM and 16GB of bootflash memory.

C8235-G2 has 16GB of DRAM and bootflash memory.

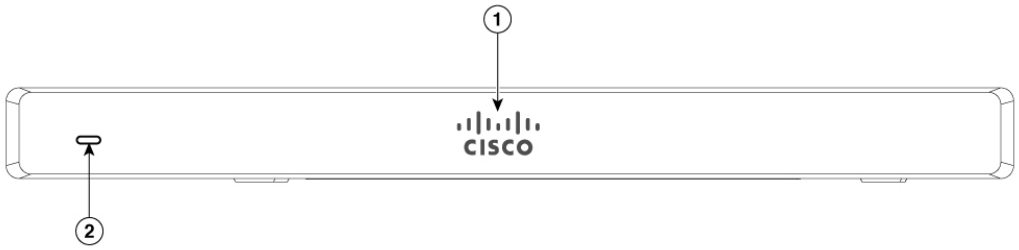
For more information on the features and specifications of Cisco 8200 Series Secure Routers, refer to Cisco 8200 Series Secure Routers datasheet.

Chassis Views

Note The compliance label is present at the bottom of the product.

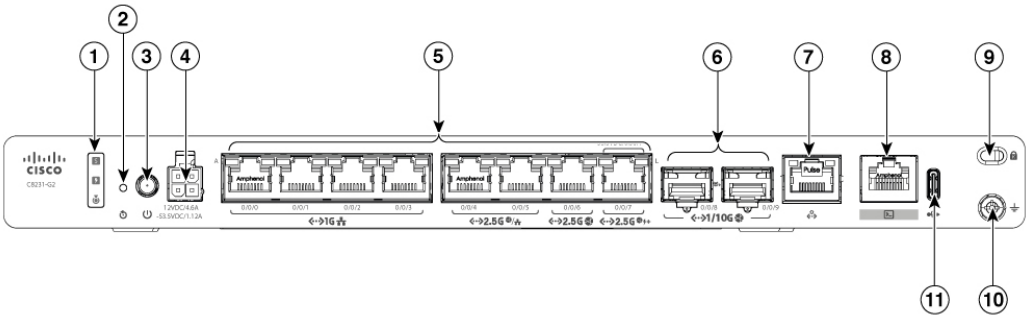
This section contains front and back panel views of the Cisco 8200 Series Secure Routers showing locations of the power and signal interfaces, interface slots, status indicators, and chassis identification labels.

Figure 1: C8231-G2 - Front View



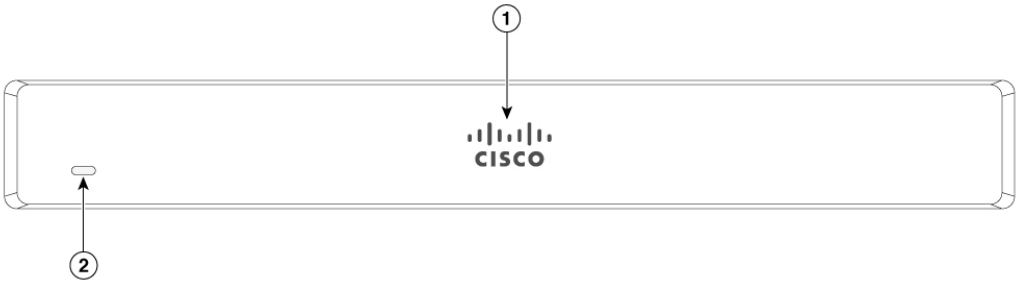
1	Non-illuminated Cisco logo	
2	Status LED	

Figure 2: C8231-G2 - I/O View



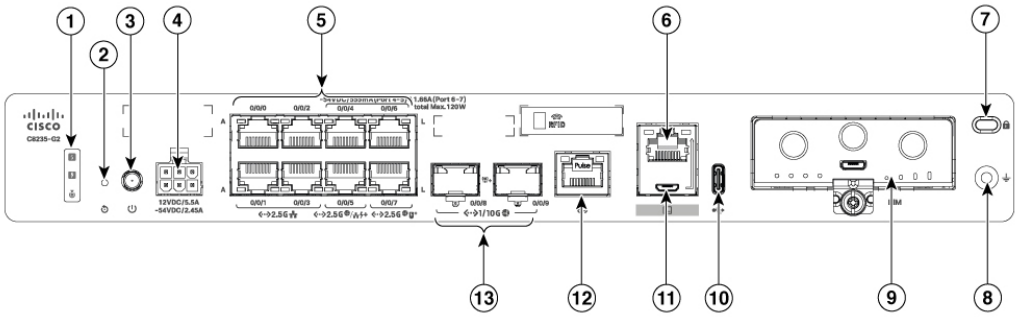
1	Status LEDs	2	Reset button
3	Power button	4	4-pin power connector
5	Ethernet ports (0-7)	6	SFP+ ports
7	Management port	8	Console port
9	Kensington lock slot	10	Ground point
11	USB Type C port		

Figure 3: C8235-G2 - Front View



1	Non-illuminated Cisco logo	
2	Status LED	

Figure 4: C8235-G2 - I/O View

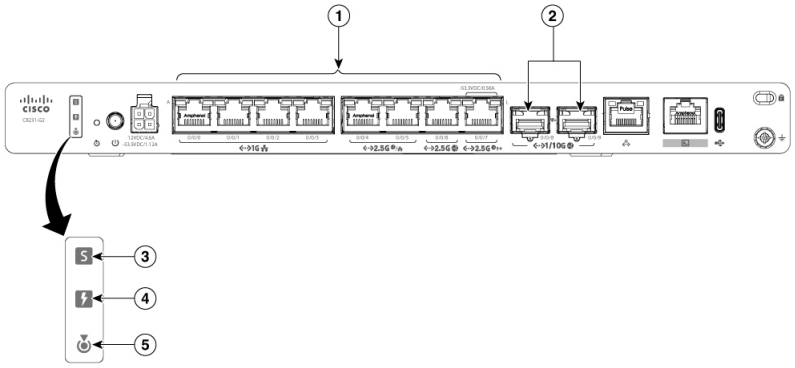


1	Status LEDs	2	Reset button
3	Power button	4	6-pin power connector
5	Ethernet ports	6	RJ45 Console port
7	Kensington lock slot	8	Ground point
9	Pluggable interface module (PIM) slot	10	USB Type C port
11	Micro-USB console port	12	Management port
13	SFP+ ports		

LED Indicators

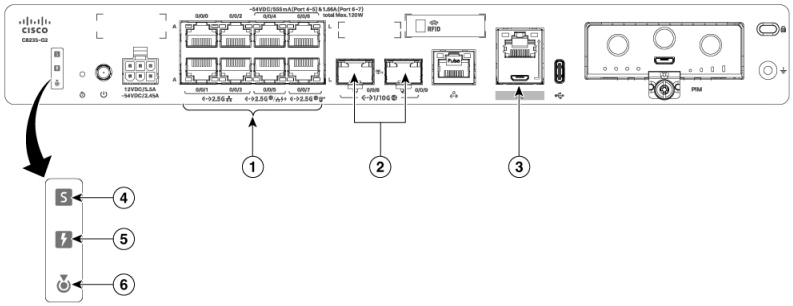
This section summarizes the LED indicators for Cisco 8200 Series Secure Routers.

Figure 5: LED Indicators C8231-G2 - I/O Side



1	Ethernet ports LED(0-7)	2	SFP port LED
3	Status LED	4	POE LED
5	Blue Beacon LED		

Figure 6: LED Indicators C8235-G2 - I/O Side



1	Ethernet ports LED 0-7 (0, 2, 4, 6 at the top and 1, 3, 5, 7 at the bottom)	2	SFP port LED
3	RJ-45 console LED	4	Status LED
5	POE LED	6	Blue Beacon LED

Table 2: LED Indicators for Cisco 8200 Series Secure Routers

Port	LED Color	Function	Description
Status (1 LED)	Tri-colour LED: Green, Amber and Red	System power status	**Off**: No power.
			Red steady on: System is booting.
			Red blink: The system has experienced a hardware integrity error.
			Amber steady on: Rommon has completed booting and system is a rommon prompt or booting IOS.
			Green steady on: Normal system operation.
POE_OK (1 LED)	Bi-colour LED: Green and Amber	POE power supply status	**Off**: No -53.5V POE power supply connected to router.
			Green Steady On: -53.5V POE power supply connected and all powered port operating normally
			Amber steady on: -53.5V POE power supply connected, but one or more POE ports has a fault.

Port	LED Color	Function	Description	
Ethernet Ports, without POE (2 LEDs per port)	Green	Activity / Link	**Left LED**: Activity	**Right LED**: Link
			Off: No data	**Off**: No link
			Green blink: Tx/Rx data	**Green steady on**:Link up
Ethernet Ports, with POE (2 LEDs per port)	Bi- colour LED Green and Amber	Activity/Link/POE status	**Left LED**: Activity	**Right LED**: Link/POE fault
			Off: No data	**Off**: No link
			Green blink: Tx/Rx data	**Green steady on**:Link up
				Amber steady on:POE fault
Console port RJ45 port/Micro USB console (1 LED)	Green	Console or AUX port function for RJ45/USB mode	**Left LED**: Integrated RJ45 Console or AUX port function enabled **Off**: USB console mode **Green on**: Console enabled	**Right LED**: Integrated RJ45 USB Mode Active **Off**:RJ45 Console /AUX Mode or nothing is connected **Green On**: USB mode
Blue beacon	Blue	Unit rack location	**Off**: Beacon not activated **On**: Beacon activated	
SFP Port 1 LED per port	Bi- colour LED Green and Amber	Link/Fault	**Off**: No link (or SFP not present) **Green**: Link up **Amber**: The SFP is not supported or it is in a fault state	

Reset Button

The actuation of the Reset button is only recognized during ROMmon boot, that is, as the router comes to the ROMmon prompt.

The Reset button does not require much force to be pressed. The Reset button should be pressed only with a small implement such as the tip of a pen or a paper clip. When the Reset button is pressed at startup, the system LED turns green.

For more information, see the Reset Overview section of the Cisco 8200 Series Secure Routers Software Configuration Guide.

Power Supply

Cisco 8200 Series Secure Routers support PoE and PoE+ power to endpoints. The product power specifications are as follows:

Power specifications for C8231-G2

- AC input voltage: Universal 100 to 240 VAC
- Frequency: 50 to 60 Hz
- Output voltage: +12VDC for system power and -53.5VDC for PoE power
- Optional PoE and PoE+ port output power: -53.5VDC, 0.56A (Port 7)
- Maximum POE port combined output power: 30W, -53.5VDC, 0.56A (Port 7)

Power specifications for C8235-G2

- AC input voltage: Universal 100 to 240 VAC
- Frequency: 50 to 60 Hz
- Output voltage: +12VDC for system power and -54VDC for PoE power
- Optional PoE and PoE+ port output power: -54VDC, 555mA (Port 4-5) and 1.66A (Port 6-7)
- Maximum POE port combined output power: 120W

Note The PoE daughter card on the C8235-G2 is included only when a PoE power supply (PSU) is selected at the time of the initial order. The PoE-DC is not field-upgradeable

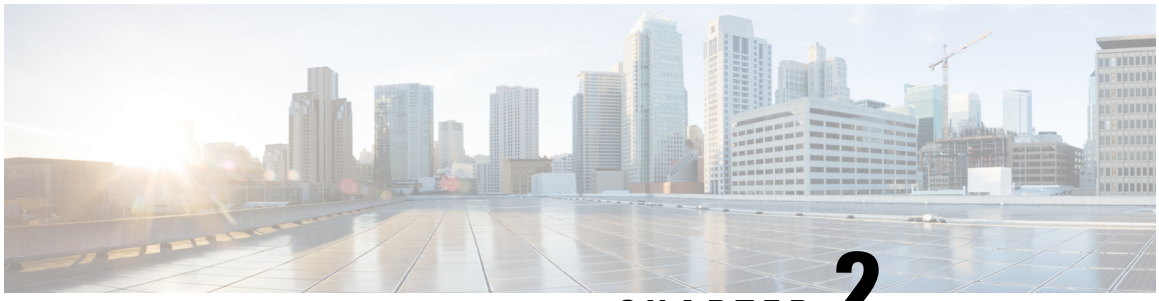
Specifications of Cisco 8200 Series Secure Routers

For specifications on the Cisco 8200 Series Secure Routers, see the Cisco 8200 Series Secure Routers' datasheet.

Periodic Inspection and Cleaning

We recommend that you periodically inspect and clean the external surface of the router. Removing is recommended to minimize the negative impact of environmental dust or debris. The frequency of inspection and cleaning is dependent upon the severity of the environmental conditions, but we recommend cleaning the router once every six months. Cleaning involves vacuuming surfaces.

Note Sites with ambient temperatures consistently above 25°C or 77°F and with potentially high levels of dust or debris might require periodic preventative maintenance cleaning.



CHAPTER 2

Prepare for Router Installation

Before you install the Cisco 8200 Series Secure Routers, you must prepare your site for the installation. This chapter provides pre-installation information, such as recommendations and requirements that should be considered before installing your router.

See the following sections to prepare for installation:

General Safety Warnings

Take note of the following general safety warnings:

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

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 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 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 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 9001—**Product Disposal

Ultimate disposal of this product should be handled according to all national laws and regulations.

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 ESD prevention procedures when removing and replacing modules:

- Ensure that the router chassis is electrically connected to 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).

Equipment Installation to Power Warnings

Take note of the following power safety warnings:

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.

Warning **Statement 1005**——Circuit Breaker

This product relies on the building's installation for short-circuit (overcurrent) protection. Ensure that the protective device is rated not greater than: 20 A

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 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 1046**—Installing or Replacing the Unit

To reduce risk of electric shock, when installing or replacing the unit, the ground connection must always be made first and disconnected last.

If your unit has modules, secure them with the provided screws.

Site selection guidelines

The Cisco 8200 Series Secure Routers require specific environmental operating conditions. Temperature, humidity, altitude, and vibration can affect the performance and reliability of the router. The following sections provide specific information to help you plan for the proper operating environment.

The Cisco 8200 Series Secure Routers are designed to meet the industry EMC, safety, and environmental standards described in the Regulatory Compliance and Safety Information for the Cisco 8200 Series Secure Routers document.

Ambient temperature

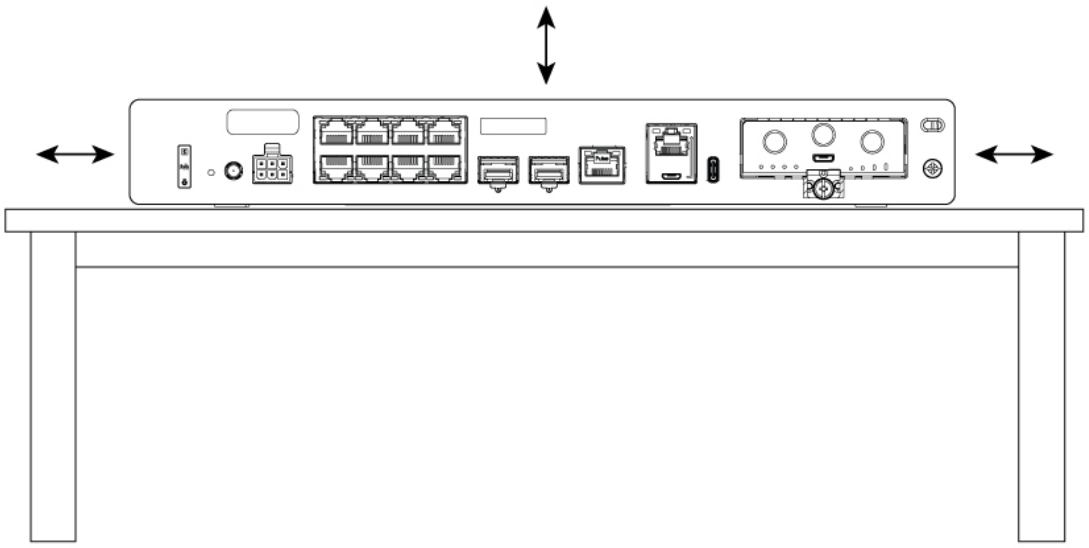
The Cisco 8200 Series Secure Router is rated for operation in an ambient environment of 40C at sea level.

- Local ambient for the router and should be measured 2” from the sides/front of the 8200 router or directly below the 8200 router when in a rack.
- The temperature should be de-rated 0.5C/1,000-feet of elevation up to 13,000 feet.

Router cooling

The Cisco 8200 Series Secure Router is Natural convection cooled (it has no fans) and requires clearance around the product. It should have at least 1.5” above and generally 1” around it on all sides. This applies to all mounting orientations.

Figure 7: Router cooling



Rack Requirements

For the Cisco 8200 Series Secure Routers, use 19-inch rack tray.

Note Rack requirements is applicable only for Cisco 8200 Series Secure Routers.

The following information can help you plan your equipment rack configuration:

- Allow clearance around the rack for maintenance.
- The Cisco 8200 Series Secure Routers requires 2RU when installed in a rack.

Note More spacing may be required depending on the installation environment.

- Enclosed racks must have adequate ventilation. Ensure that the rack is not congested because each router generates heat. An enclosed rack should have louvered sides and a fan to provide cooling air. The heat generated by the equipment near the bottom of the rack can be drawn upward into the intake ports of the equipment above it.

Power Guidelines and Requirements

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

This section lists the power requirements for the Cisco 8200 Series Secure Routers.

Table 3: Power Requirements for C8231-G2

Power Source	Input Rated	Output Rated
66W AC Power Adapter (PWR-CC1-66WAC)	100-240V, <=2A	12 VDC, 5.5A
115W AC Power Adapter (PWR-CC1-115WAC)	100-240V, <=1.8A	12V, 4.6A, -53.5V 1.12A

Table 4: Power Requirements for C8235-G2

Power Source	Input Rated	Output Rated
66W AC Power Adapter (PWR-CC2-66WAC)	100-240V, <=2A	12VDC, 5.5A
230W AC Power Adapter (PWR-CC1-230WAC)	100-240V, <=3.2A	12V, 9.0A; -54V, 2.45A

Network Cabling Specifications

The following sections describe the cables and the specifications required to install Cisco 8200 Series Secure Routers:

Console Port Considerations

The router includes an asynchronous serial console port. The console ports provide access to the router using a console terminal connected to the console port. This section discusses important cabling information to consider before connecting the router to a console terminal or modem.

Console terminals send data at speeds slower than modems do; therefore, the console port is ideally suited for use with console terminals.

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. Only one port can be used at the same time.

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. For detailed information about installing a console terminal, see the Connecting to a Console Terminal or Modem section.

For cable and port pinouts, see the Cisco Modular Access Router Cable Specifications document located on Cisco.com.

USB Serial Console

The USB serial console port connects directly to the USB connector of a PC using a USB Type A to 5-pin micro USB Type-B cable. The USB Console supports full speed (12Mb/s) operation. The console port does not support hardware flow control.

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

USB Console OS Compatibility

- Windows 10, Windows 8, Windows 7, Windows 2000, Window XP 32 bit, Windows Vista 32 bit
- 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

The default parameters for the console port are 9600 baud, 8 data bits, no parity, and 1 stop bit. For detailed information about installing a console terminal, see the Connecting to a Console Terminal or Modem section on page 3-19.

For operation with a Microsoft Windows OS version older than Windows 7, the Cisco Windows USB Console Driver must be installed on any PC connected to the console port. If the driver is not installed, the prompts guide you through a simple installation process.

The Cisco Windows USB Console Driver allows plugging and unplugging the USB cable from the console port without affecting Windows HyperTerminal operations. No special drivers are needed for Mac OS X or Linux.

Only one console port can be active at a time. 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.

Note Only the 5-pin micro USB Type-B is supported.

Prepare for Router Installation

Before you install the Cisco 8200 Series Secure Routers, you must prepare your site for the installation. This chapter provides pre-installation information, such as recommendations and requirements that should be considered before installing your router.

See the following sections to prepare for installation:

Ethernet Connections

The IEEE has established Ethernet as standard IEEE 802.3. The routers support the following Ethernet implementations:

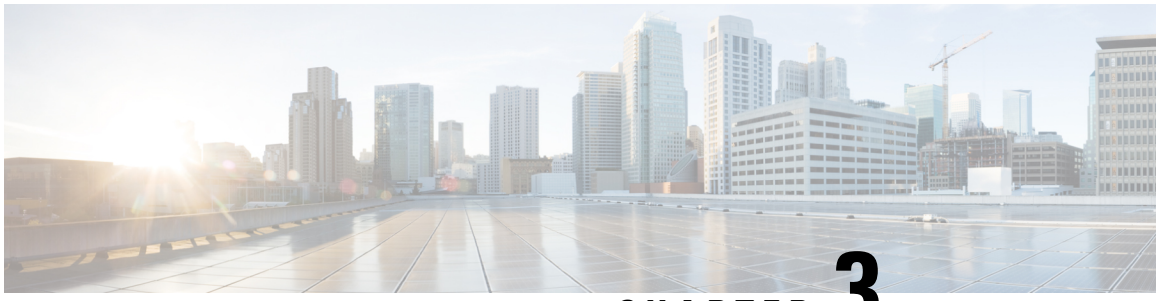
1000BASE-T—1000 Mb/s full-duplex transmission over a Category 5 or better unshielded twisted-pair (UTP) cable.	Supports the Ethernet maximum length of 328 feet (100 meters).
100BASE-T—100 Mb/s full-duplex transmission over a Category 5 or better unshielded twisted-pair (UTP) cable.	Supports the Ethernet 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).
2.5GBASE-T – 2.5 Gb/s full-duplex transmission over a Category 5e or better unshielded twisted-pair (UTP) cable.	Supports the Ethernet maximum length of 328 feet (100 meters).

See the Cisco Modular Access Router Cable Specifications document at Cisco.com for information about Ethernet cables, connectors, and pinouts.

Required Tools and Equipment for Installation and Maintenance

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

- An ESD-preventive cord and a wrist strap
- A number 2 Phillips screwdriver
- Phillips screwdrivers: small, 3/16-in. (4 to 5 mm) and medium 1/4-in. (6 to 7 mm). You might need these when you install or remove modules, and when you remove the cover (when you upgrade the memory or other components)
- Screws that fit your rack
- A wire crimper
- A wire for connecting the chassis to an earth ground: AWG 14 (2 mm^2) or larger wire
- An appropriate user-supplied UL or a CSA-certified ring terminal with an inner diameter of 1/4 in. (5 to 7 mm)



CHAPTER 3

Install and Connect the Router

This chapter describes how to install and connect Cisco 8200 Series Secure Routers to LAN and WAN networks.

Unpack the Router

Unpack the router only when you are ready to install it. If the installation site is not ready, to prevent accidental damage, keep the chassis in its shipping container until you are ready to install.

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

Set up Router on Desktop, Rack, Wall, Under-desk or DIN-rail mount

After unpacking, based on your requirements, you can set up a Cisco 8200 Series Secure Routers on a desktop, a rack, a wall, a Din-Rail or under a desk.

Note You can install external modules before or after mounting a router. However, if you choose to install the external modules after mounting the router on the rack or wall, ensure that you have optimal access to the back/front panel of the router.

For information on modules and Field Replaceable Units (FRUs), see the Install and Upgrade FRUs section.

The available options for mounting a Cisco 8200 Series Secure Routers are:

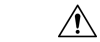
Table 5: Models and Mounting Options

Model	Mounting Options
C8231-G2	Desktop, Rack Mount, Wall Mount using Key-hole Slots, Din-Rail, Under-desk
C8235-G2	Desktop, Rack Mount, Wall Mount using Key-hole Slots, Din-Rail, Under-desk

If you choose to setup the router on a desktop, you can place the router on a desktop, bench top or on a shelf.

Mount the router on a desk

You can mount the chassis on a desktop by placing it on a desk in a horizontal position. Make sure there are no blockages or obstructions within one inch of the top of the chassis or within 0.5 inches of the sides so that nothing interferes with cooling.

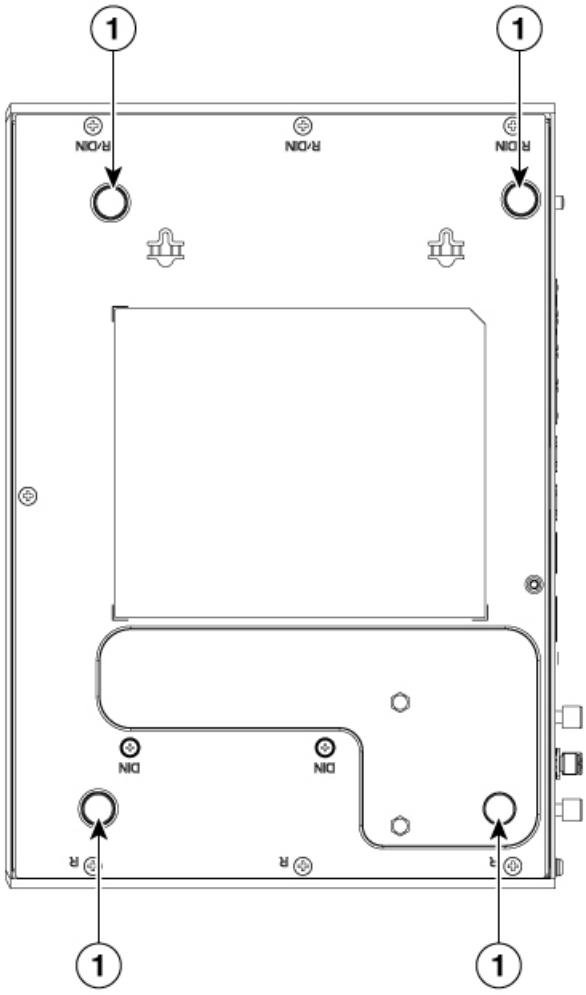


Caution Do not stack multiple Cisco 8200 Series Secure Routers when mounting the routers on a table top.

Do not put any object on the sides or on top of the routers ensuring that there is ample space for air circulation and heat removal.

The bottom of the router has four rubber feet that protect the router and the surface. Do not remove the rubber feet included with the chassis. They are needed for proper cooling.

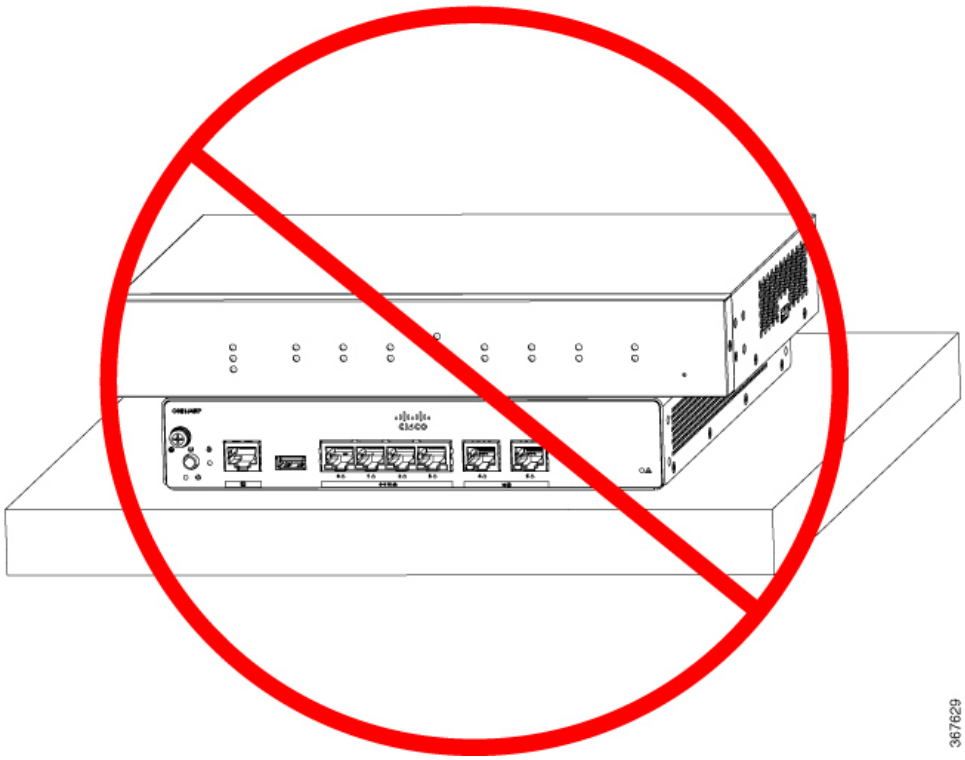
Figure 8: Rubber feet for C8235-G2 Routers



1.	Rubber feet

Note Do not stack routers.

Figure 9:



Rack Mount

Before mounting the router on to the rack, refer to the following safety warning statements:

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.

Important

Periodic Inspection and Cleaning: We recommend that you periodically inspect and clean the external surface of the router. Removing is recommended to minimize the negative impact of environmental dust, debris, and liquid contamination. The frequency of inspection and cleaning is dependent upon the severity of the environmental conditions, but we recommend cleaning the router once every six months. Cleaning involves vacuuming router air intake and exhaust vents.

Note Using the top plate on the chassis significantly helps in preventing any damages that may occur from rodent infestation.

Note Sites with ambient temperatures consistently above 25°C or 77°F and with potentially high levels of dust or debris might require periodic preventative maintenance cleaning.

Note When mounting Cisco 8200 Series Secure Routers on a rack, ensure that there is ample surrounding space. This ensures more heat removal, which in turn helps the surrounding air temperature to stay within the specified operating conditions.

Rack Mount C8231-G2

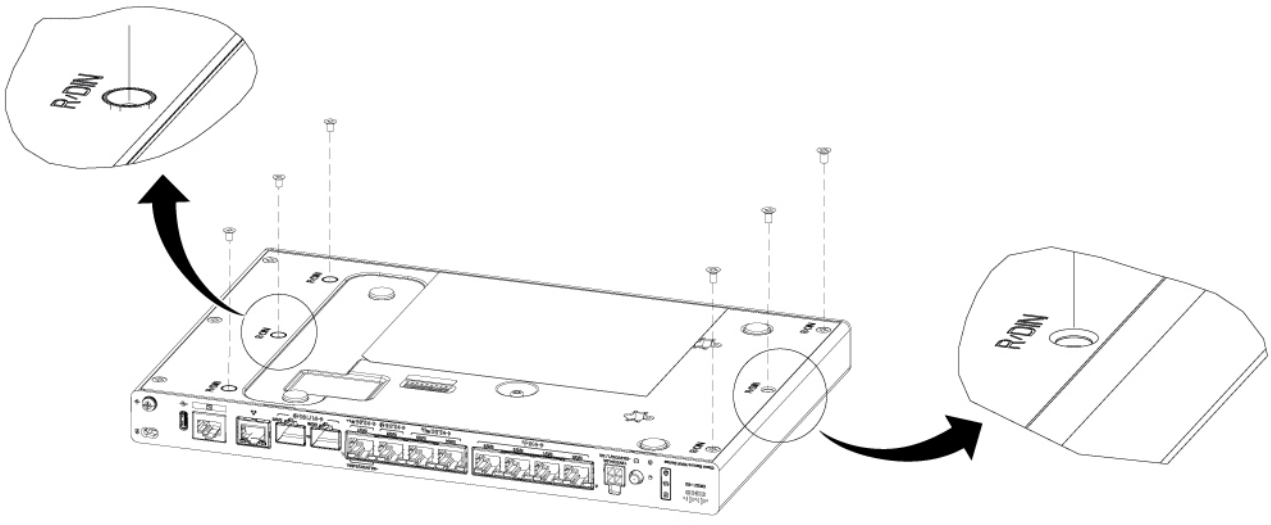
This procedure describes how to rack mount the router:

Procedure

Step 1 Remove six screws from the holes marked with an “R” from bottom of the router. Ensure you keep them as they will be used to secure the router to the rack-tray.

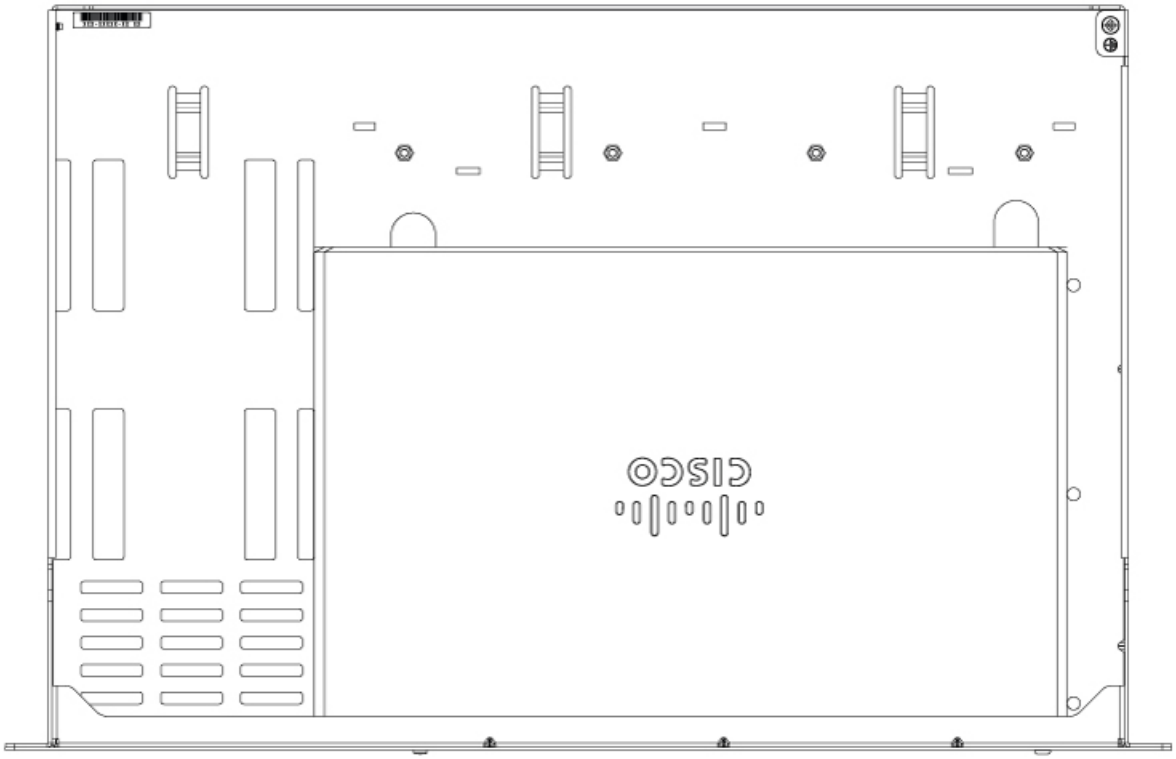
Note
Three of the screws are black in colour and need to be reassembled to the locations where they were removed.

Figure 10:



Step 2 Locate the I/O end of the router and place it facing the front of the rack-tray.

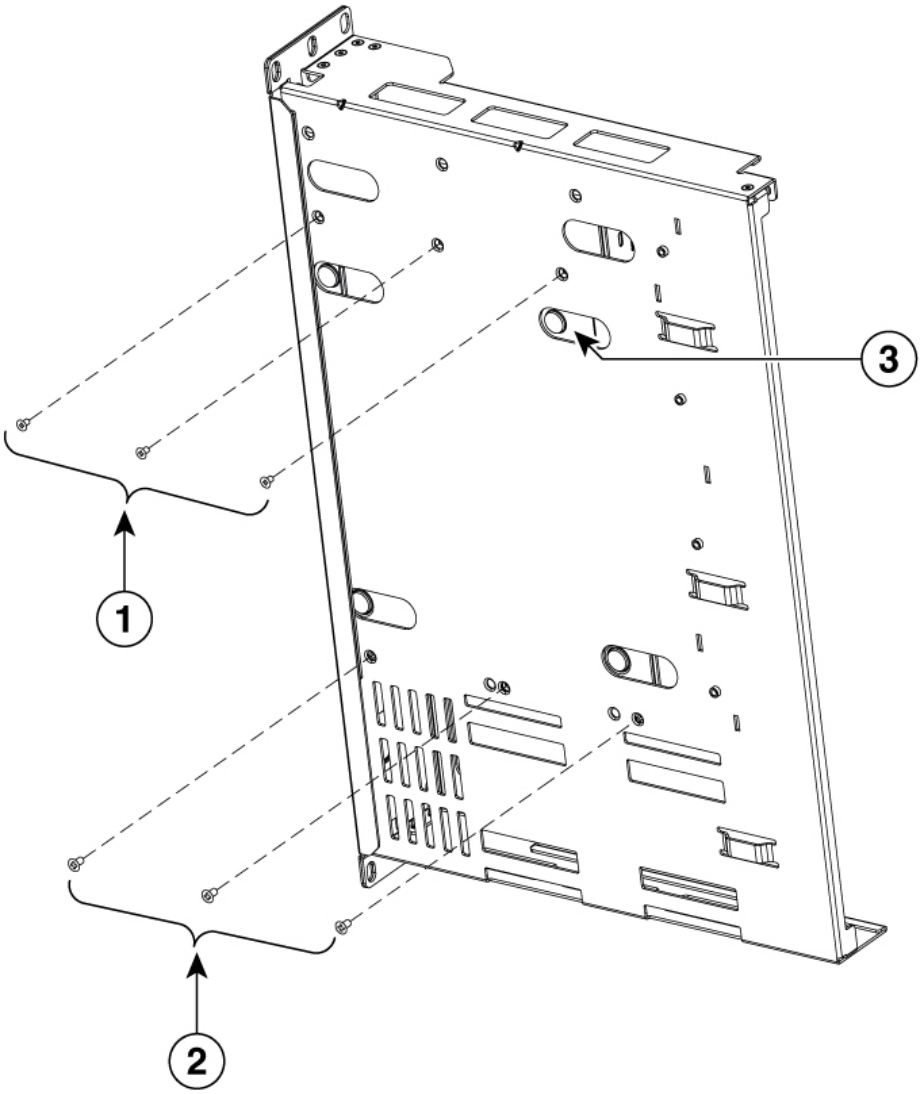
Figure 11: Place the router on the rack-tray



Step 3 Ensure that the rubber mounting feet are contained in the open slots. Retrieve the six screws that were removed from the router base and install them back through the holes in the rack-tray to secure the router to the tray. Ensure that the black screws are back in the same location.

Note
The screw locations will line up, when the rubber mounting feet are correctly placed in their slots.

Figure 12: Secure router to rack tray (C8231-G2)

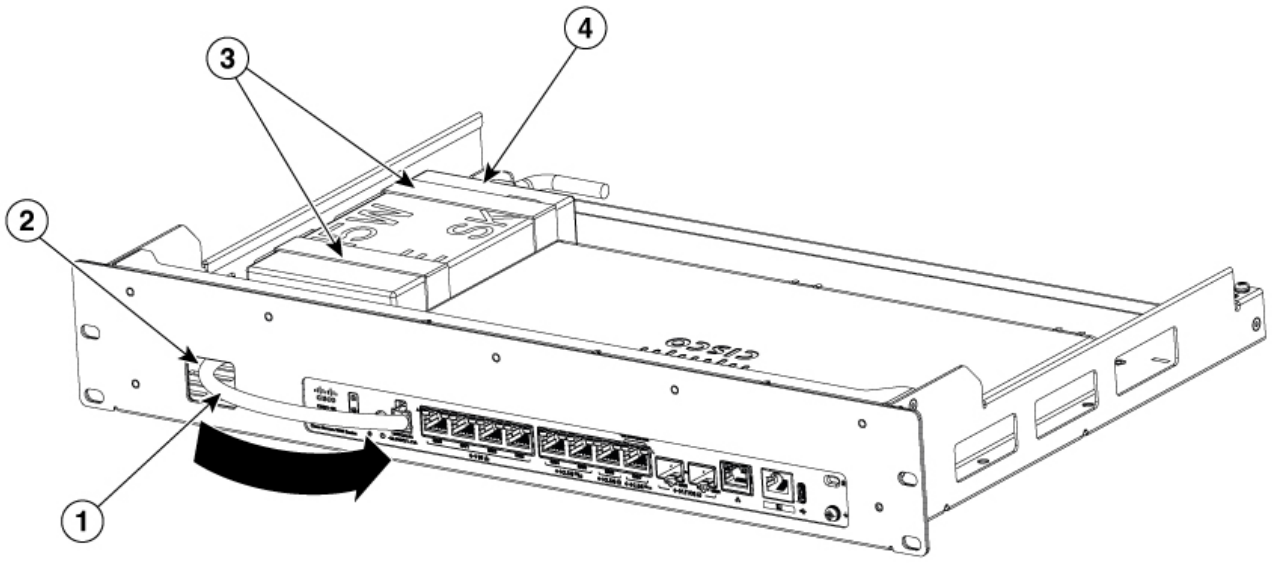


1	Router screws originally removed from the base (black, M3)
2	Router screws originally removed from thr base (silver, #6-32)
3	Rubber mounting feet in rack-tray slots. (one location shown)

Step 4 Route the power supply cable through the cabling-cutout in the front panel. Place the Power Supply Units (PSU) in the tray.

Note
Power Supply Units (PSU) vary in size from small to large. Secure the PSUs to the rack-tray using different sizes of velcro strap pairs by using the slots in the rack-tray. Use a Tywrap to bundle the cabling at the front of the tray and secure it to the tray.

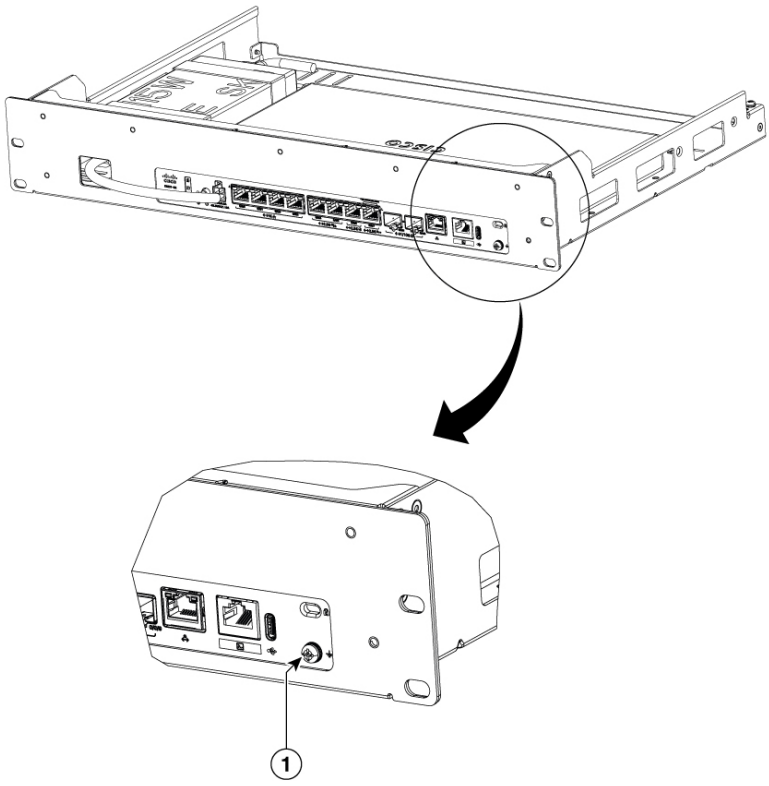
Figure 13: Place the power supply unit in the tray



1	Power supply cable
2	Cabling-cutout in front panel
3	Velcro straps
4	Power supply body

Step 5 The ground location for the router is located on the front face and accessible through the rack-tray panel.

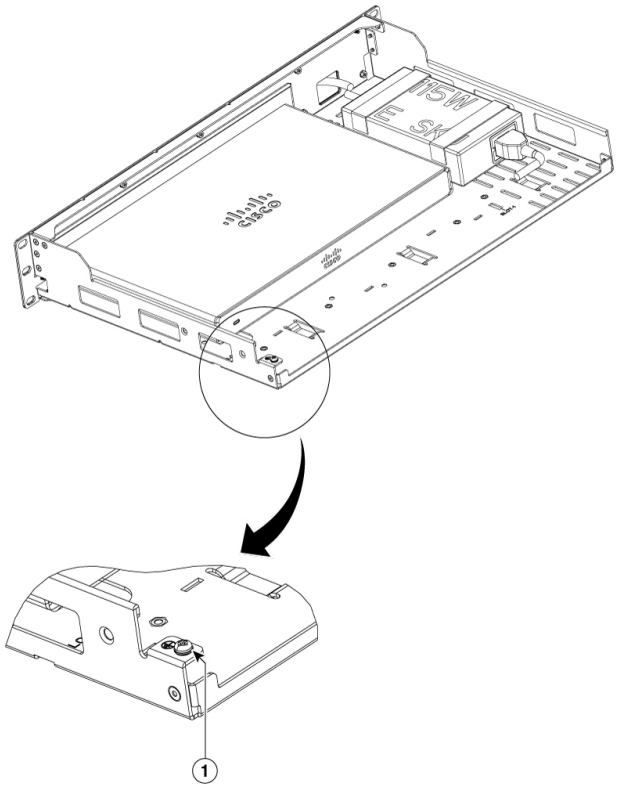
Figure 14: Ground option on the front side of the tray



1	Ground location at front of router

A grounding location of the same screw size is provided on the rear of the rack-tray if it is preferred instead of using the ground location at the front of the router. For more information see, the Chassis Grounding section.

Figure 15: Ground option on the rear end of the tray

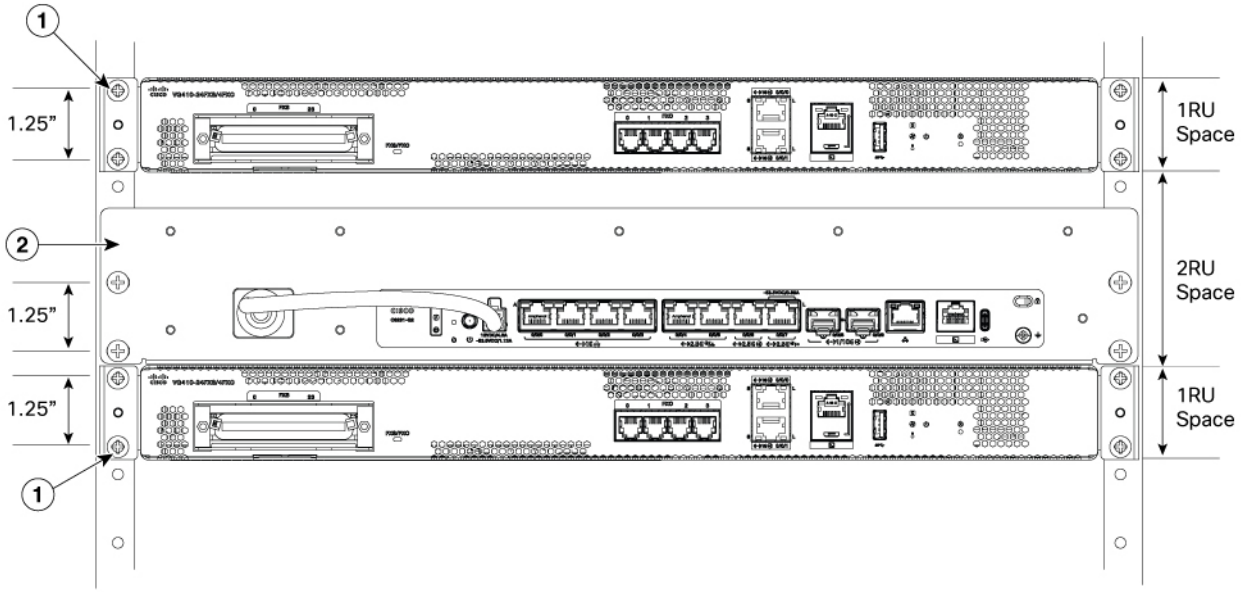


1	Ground location at back of the tray

Step 6 Install the rack-tray assembly into the rack by aligning the bottom of the rack-tray to the bottom of the Equipment Racks Rack-Unit (RU) spacing and secure the screws.

Note
Rack-tray is shorter than 2RU tall, but must be allocated the full 2RU of space.

Figure 16: Rack-tray assembly



1	Typical 1RU product (reference only)
2	Rack-tray installed

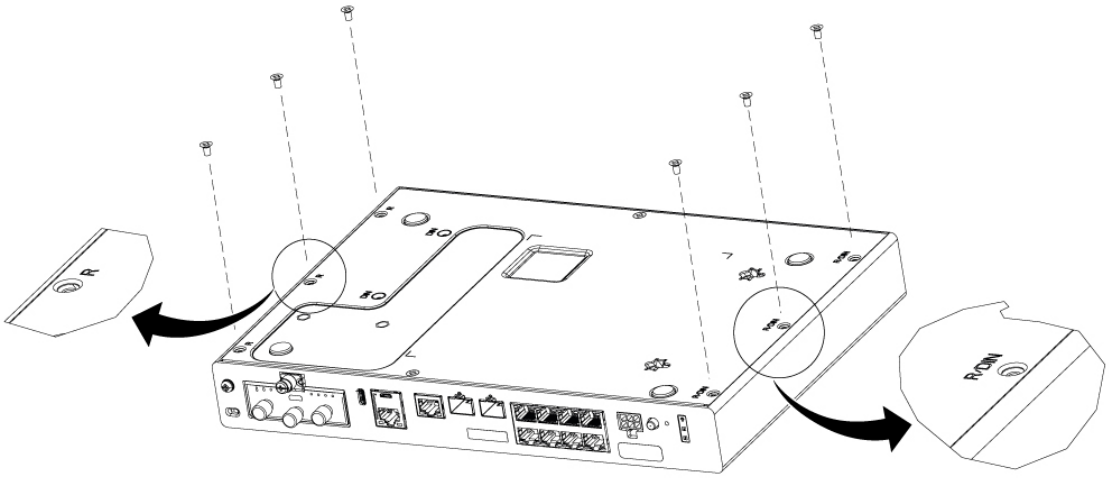
Rack Mount the C8235-G2

This procedure describes how to rack mount the router chassis:

Procedure

Step 1 Remove six screws from the holes marked with an “R” from bottom of the router. Ensure you keep them as they will be used to secure the router to the rack-tray.

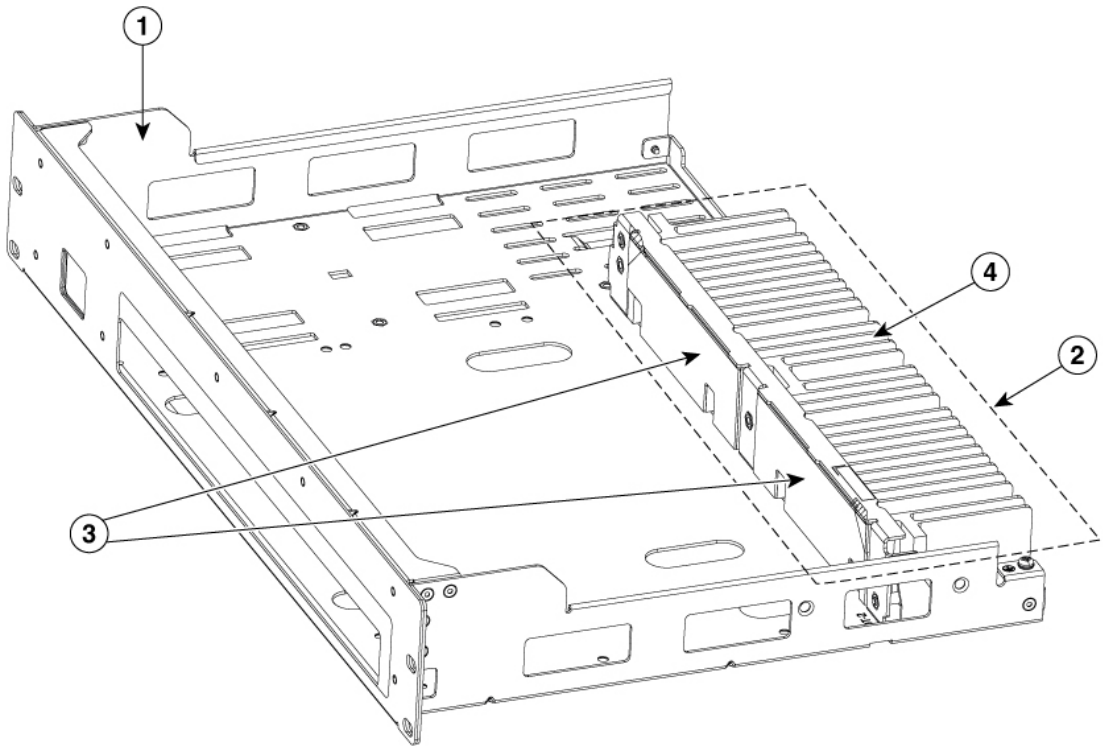
Figure 17: Locate the screws on the router



Step 2 The heatsink-assembly is fixed to the rack-tray. The heatsink is free to move on guide-pins within the heatsink-assembly. This is so the heatsink can be moved out of the way to allow clearance for installing the router and prevent damage to the thermal interface before attaching the heatsink-assembly to the router.

Note
C8235-G2 Rack-trays comes with a heatsink-assembly. This provides required cooling to the router to operate over the full temperature range when installed in a rack.

Figure 18: Heatsink-assembly

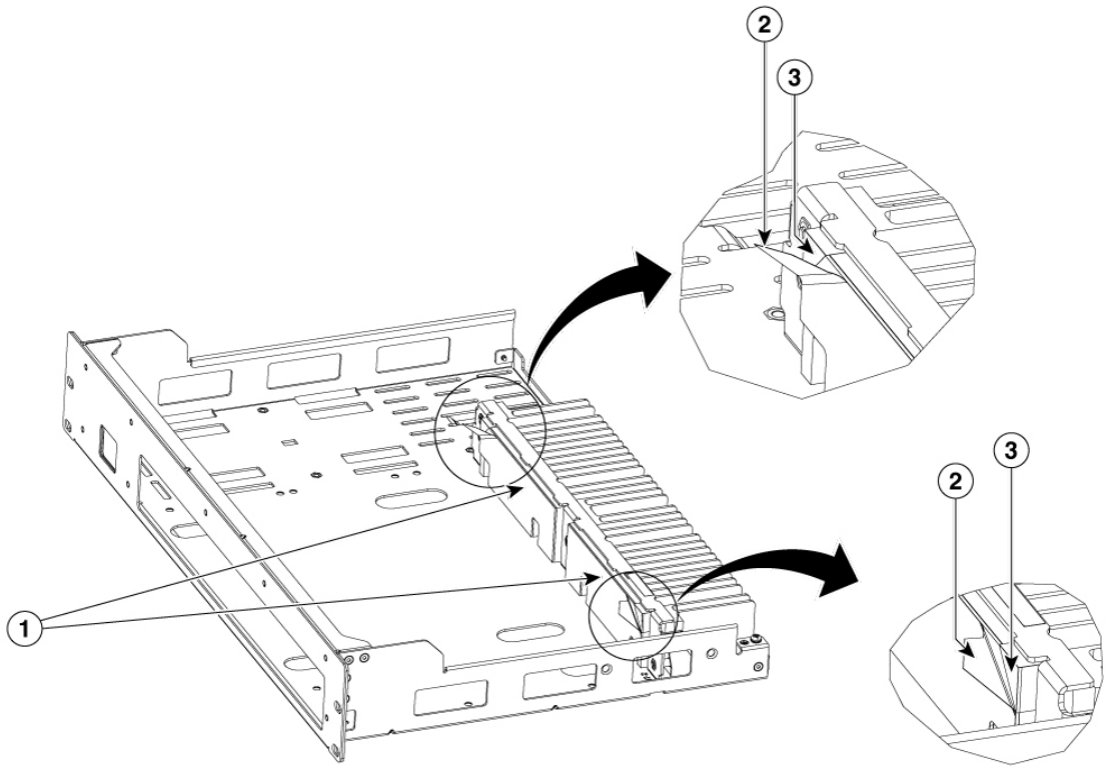


1	Rack-Tray
2	Heatsink assembly
3	2X Thermal interfaces on heatsink
4	Heatsink

Step 3 Peel off the protective-liner from both thermal interfaces on the heatsink, one corner at a time as shown in the figure, so that the thermal interface stays adhered to the heatsink.

Note
Ensure that the heatsink liner is removed for correct functioning of the heatsink.

Figure 19: Protective layer of heatsink-assembly

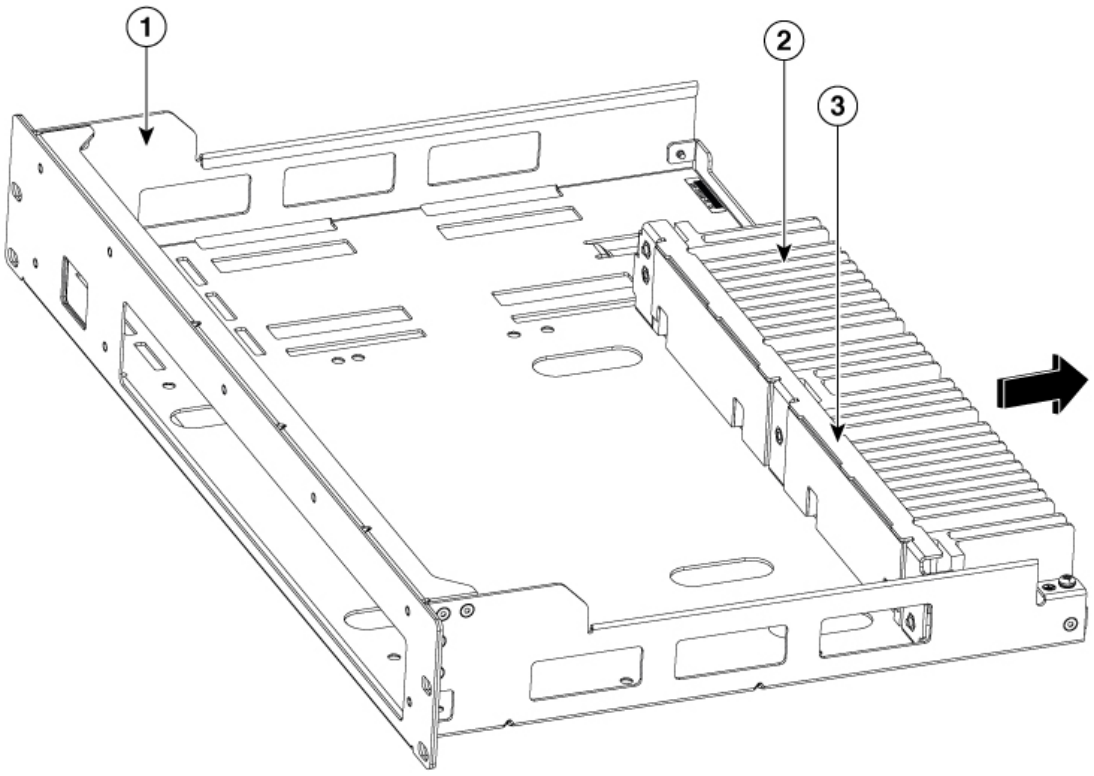


1	2X Thermal Interfaces on heatsink
2	Thermal interface protective liner
3	Thermal interface on heatsink base with liner removed

Step 4 Slide the heatsink back as far as it will go on the guide-pins.

Note
The heatsink metal frame is the part of the heatsink-assembly that remains secured to the rack-tray.

Figure 20: Heatsink metal frame



1	Rack-tray
2	Heatsink
3	Heatsink assembly metal frame

Step 5 Locate the front end (I/O) of the router and place it at an angle at the front of the rack-tray. Lower the rear end of the router down into the rack-tray carefully not to damage the thermal interface on the heatsink base.

Figure 21: Router placement on rack tray

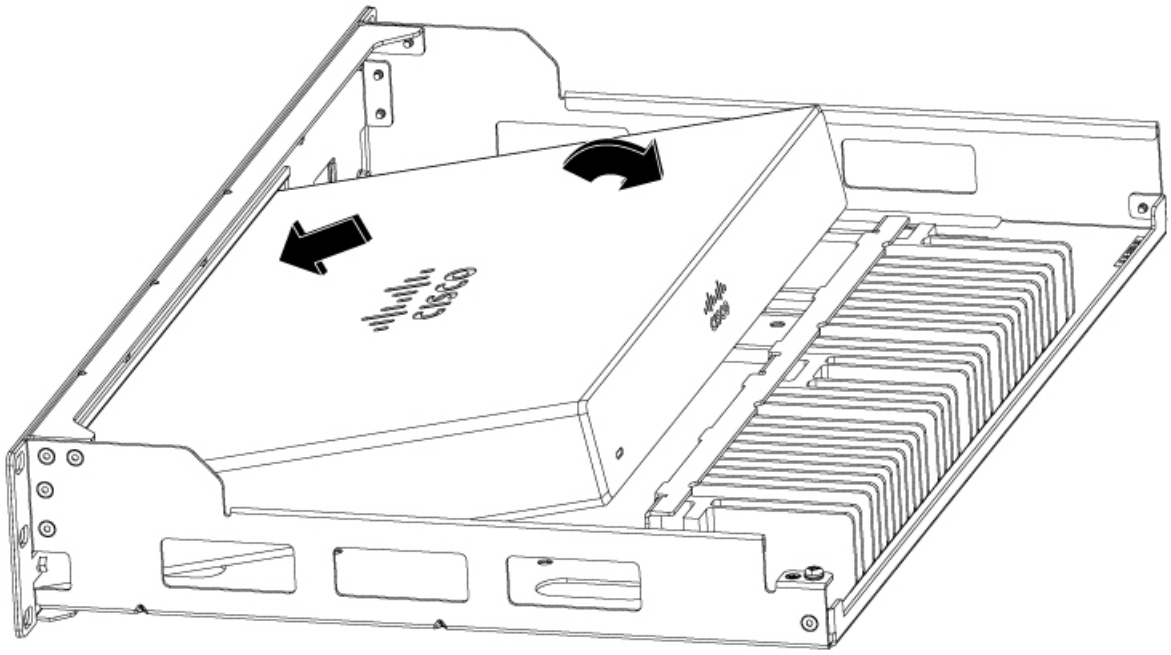
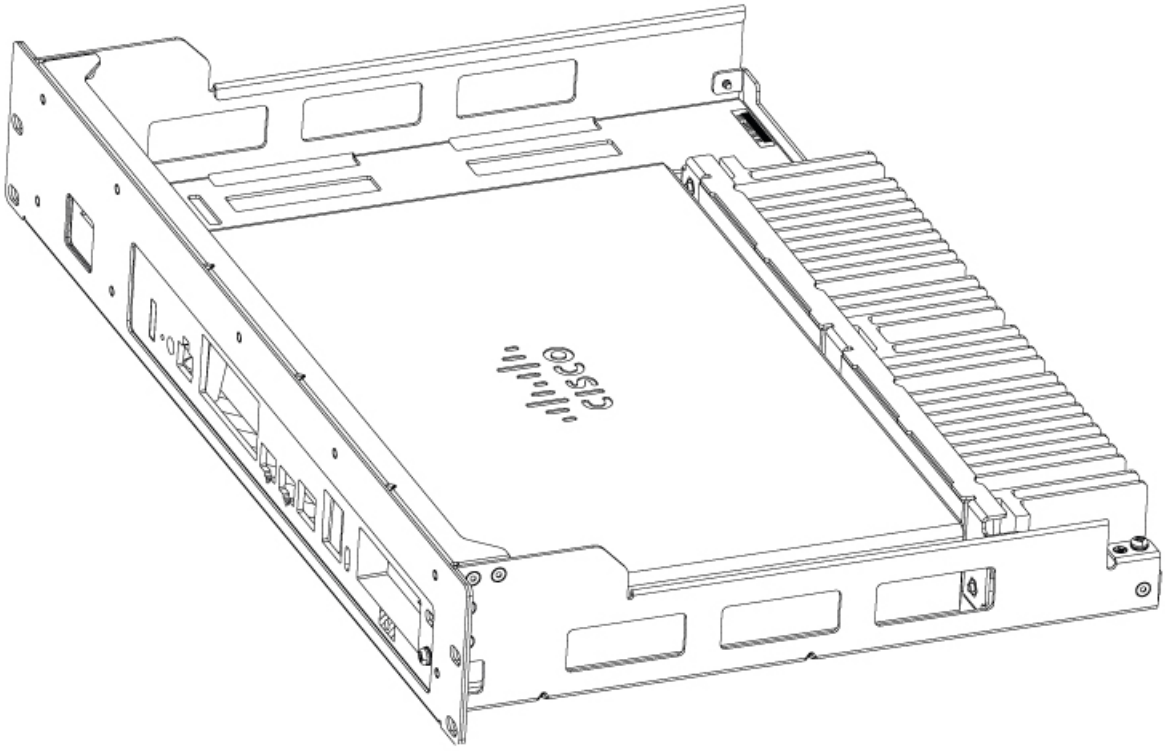


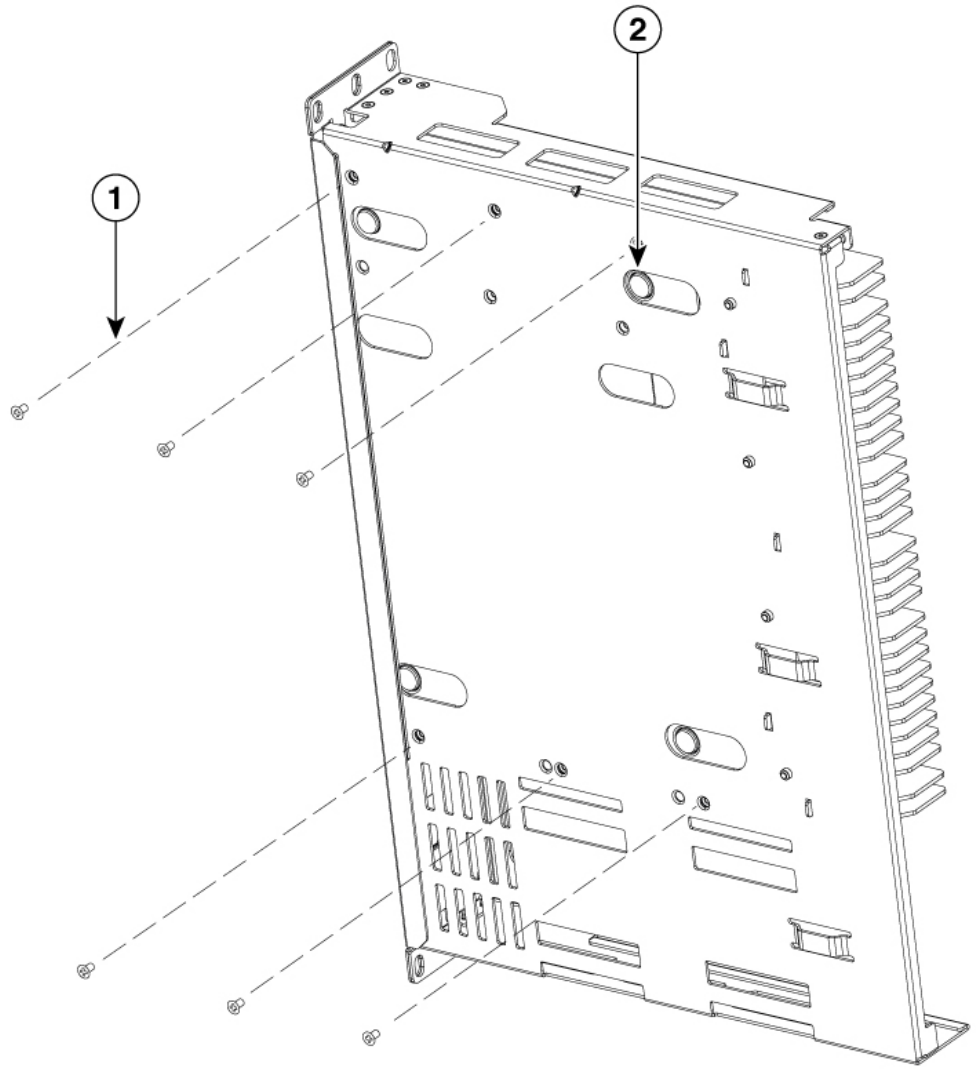
Figure 22: Router placed on the rack tray



Step 6 Ensure that the rubber mounting feet are contained in the open slots. Retrieve the six screws that were removed from the router base and install them back through the holes in the rack-tray to secure the router to the tray.

Note
The screw locations will line when the rubber mounting feet are correctly placed in their slots.

Figure 23: Secure router to the tray



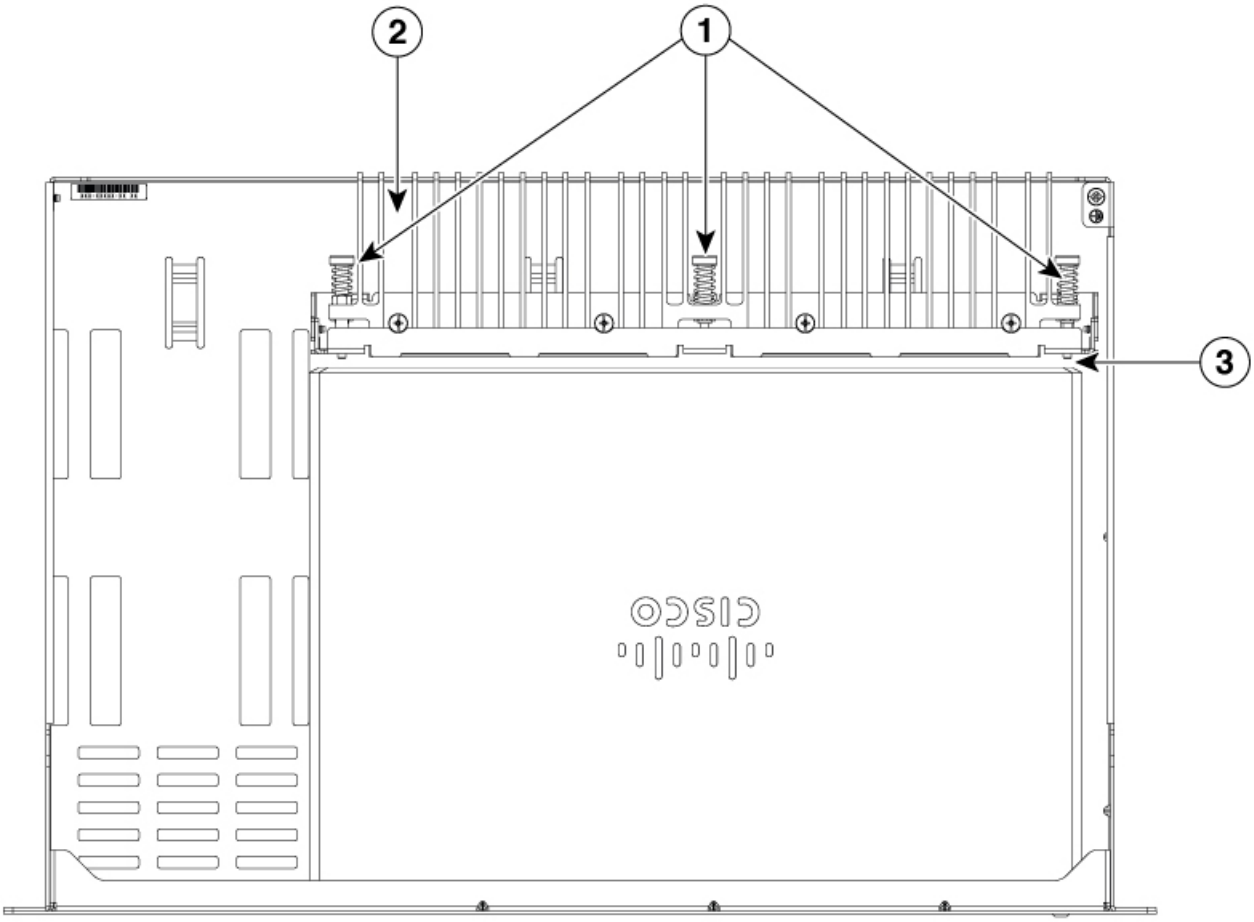
1	Router screws originally removed from the base
2	Rubber mounting feet in rack-tray slots. (one location shown).

Step 7 Secure the heatsink correctly to provide the required cooling for the router. Once the router is secured to the Rack-tray, there will be a gap between the heatsink and the back of the router.

Note

The heatsink does not secure to the router itself. When secured, the clamping pressure of the spring-screws within the heatsink assembly establishes contact of the heatsink to the router.

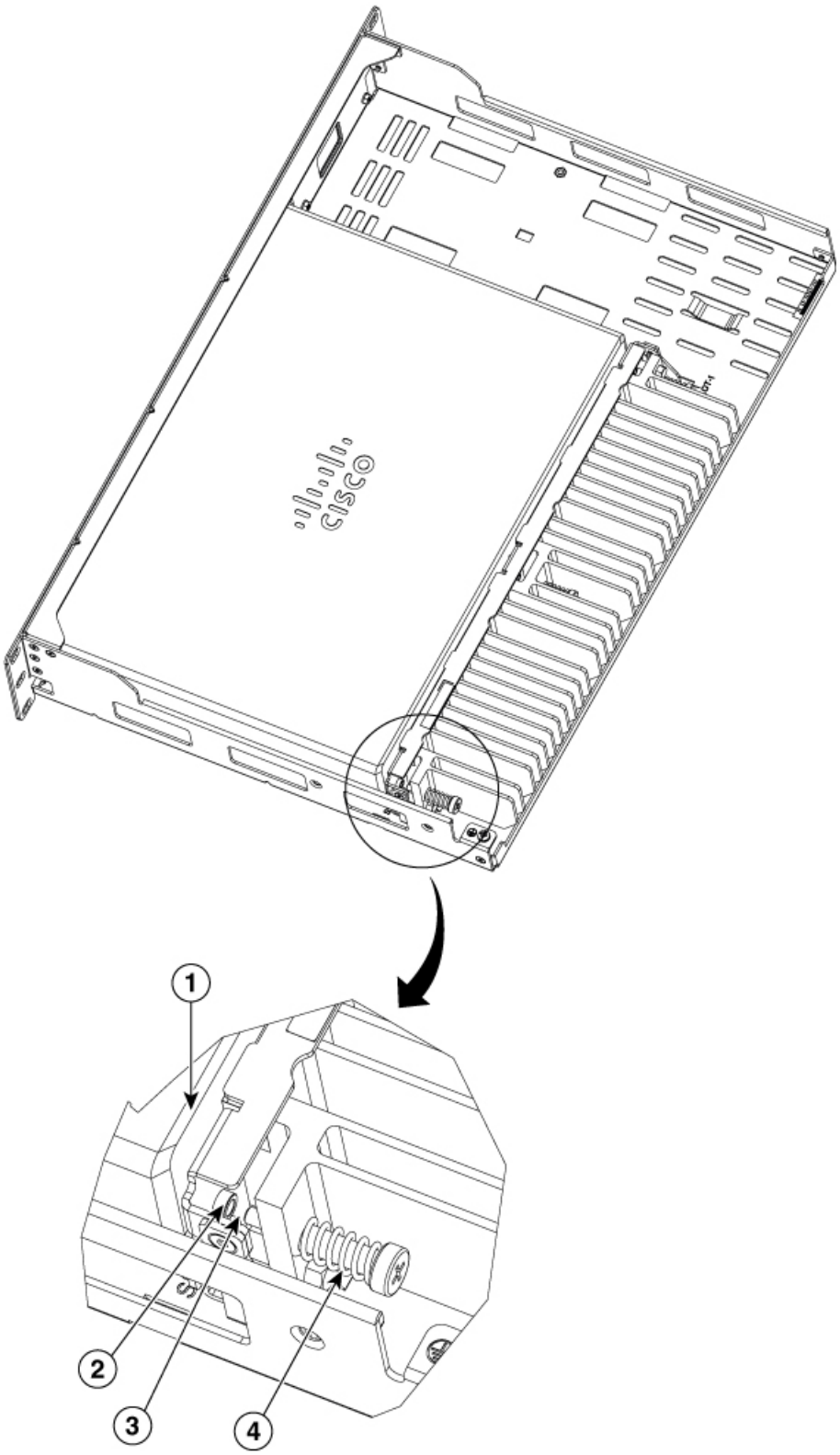
Figure 24: Secure heatsink



1	Spring-screws (3)
2	Heatsink
3	Gap between Heatsink and the router after the router installation

The heatsink has three captive spring-screws that need to secure to the heatsink frame so that the heatsink makes contact with the router. When the heatsink is slid backwards, there is a gap between the (3) spring-screws and the securing nut in the heatsink-assembly.

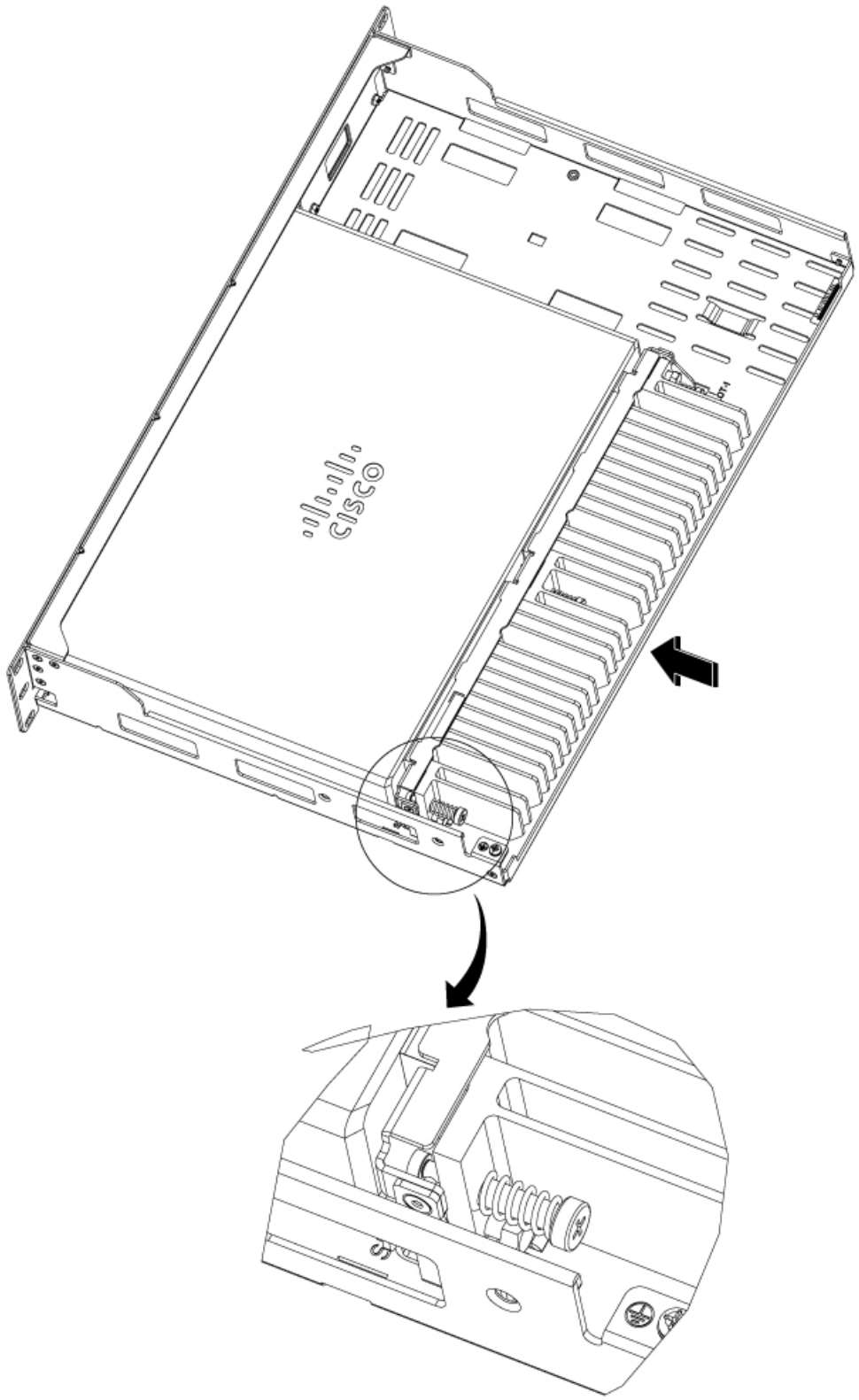
Figure 25:


1
2
3
4

1	Contact of Heatsink to the router
2	Securing nut in heatsink assembly
3	Small gap to spring screw
4	Spring-screw

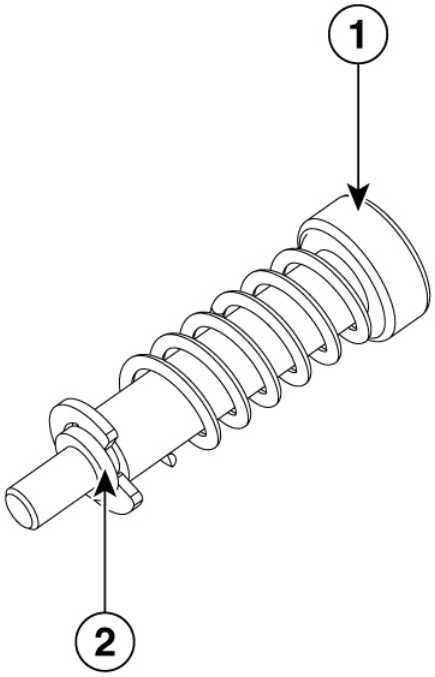
Step 8 Slide the heatsink until it is in contacts the router. There may still be a very small gap between the spring-screw threads and securing nut on the heatsink-assembly.

Figure 26:



Step 9 Tighten the spring-screw until the shoulder of the spring-screw bottoms on the securing nut.

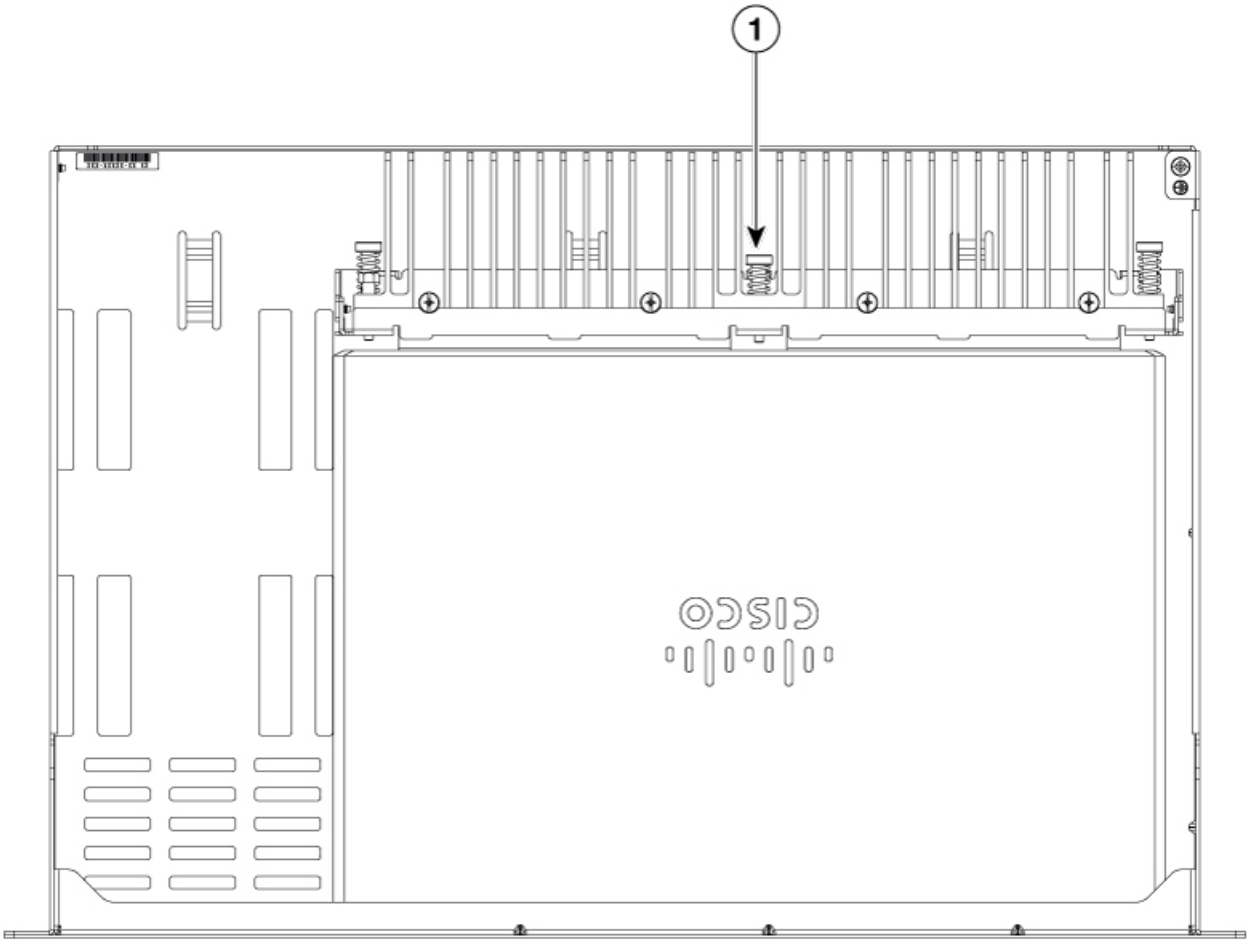
Figure 27: Spring-screw



1	Spring-screw
2	Shoulder of the spring-screw

Secure middle spring-screw.

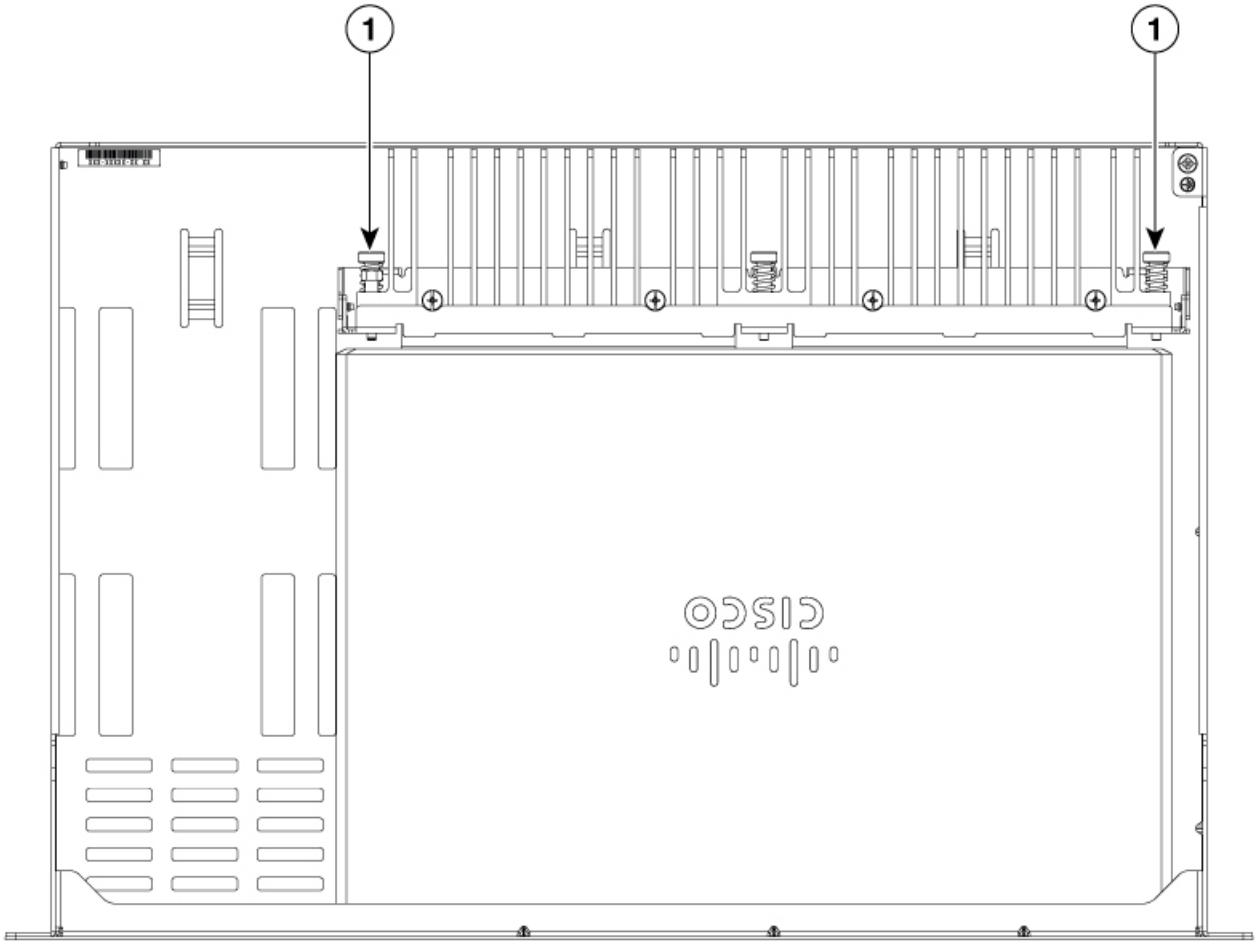
Figure 28: Middle spring-screw



1	Middle spring-screw

Secure outer spring-screws.

Figure 29: Outer spring-screw

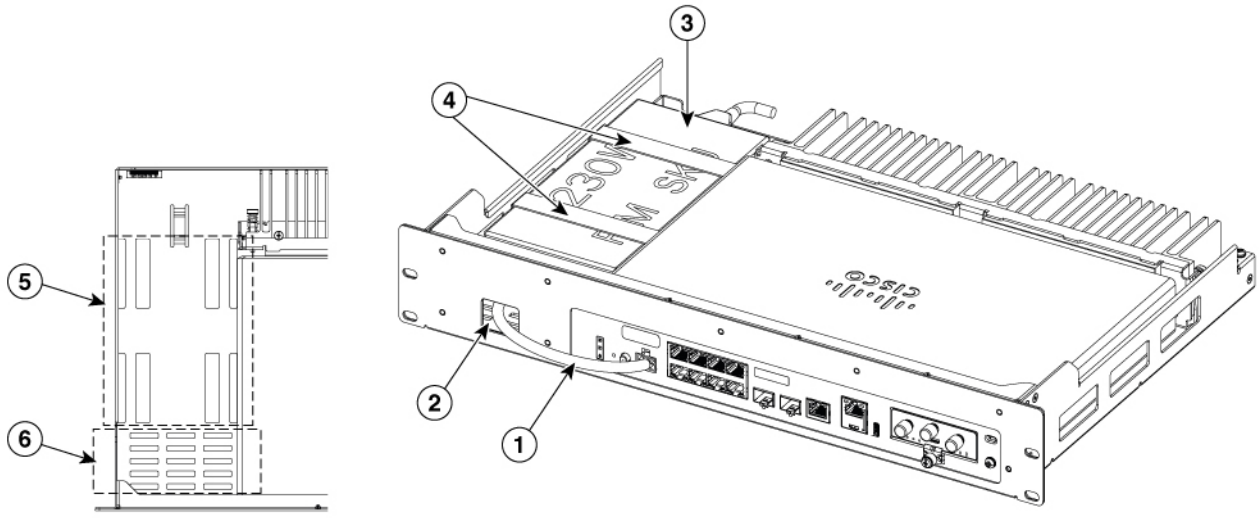


1	Outer spring-screws

Step 10 Route the power supply cable through the cabling-cutout in the front panel. Place the Power Supply Units (PSU) in the tray.

Note
Power Supply Units (PSU) vary in size from small to large. Secure the PSUs to the rack-tray using different sizes of velcro strap pairs by using the slots in the rack-tray. Use a Tywrap to bundle the cabling at the front of the tray and secure it to the tray.

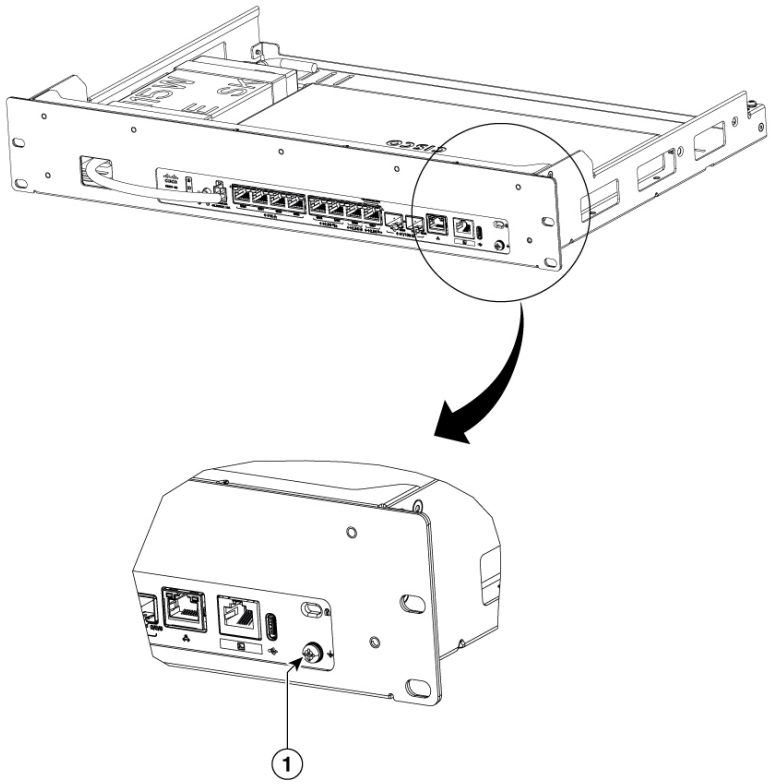
Figure 30: Place the power supply unit in the tray



1	Power supply cable
2	Cabling-cutout in the front panel
3	Power supply unit
4	Velcro straps
5	Slots in the Rack-tray for velcro-strap securing of PSU
6	Slots in the Rack-tray for tywrap securing of excess cable

Step 11 The ground location for the router is located on the front face and accessible through the rack-tray panel.

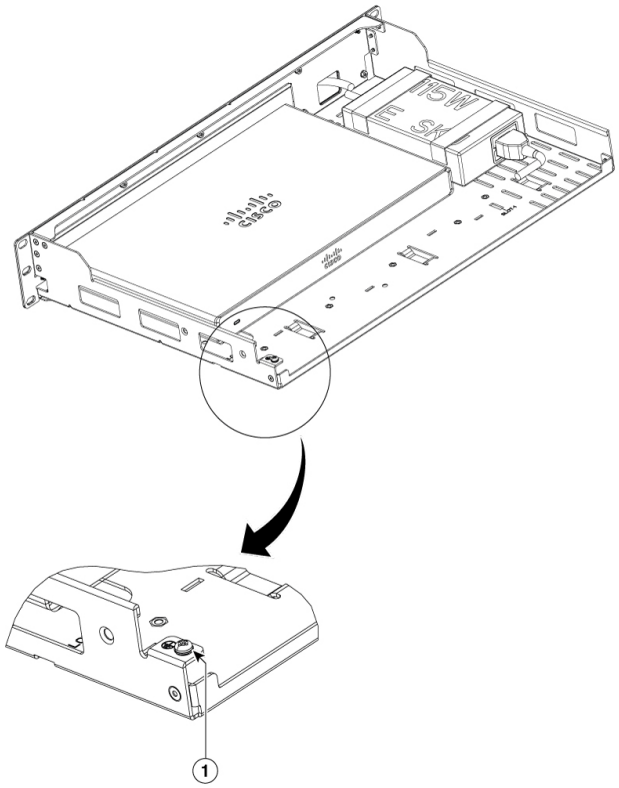
Figure 31: Ground option on the front side of the tray



1	Ground location at front of router

A grounding location of the same screw size is provided on the rear of the rack-tray if it is preferred instead of using the ground location at the front of the router. For more information see, the Chassis Grounding section.

Figure 32: Ground option on the rear end of the tray

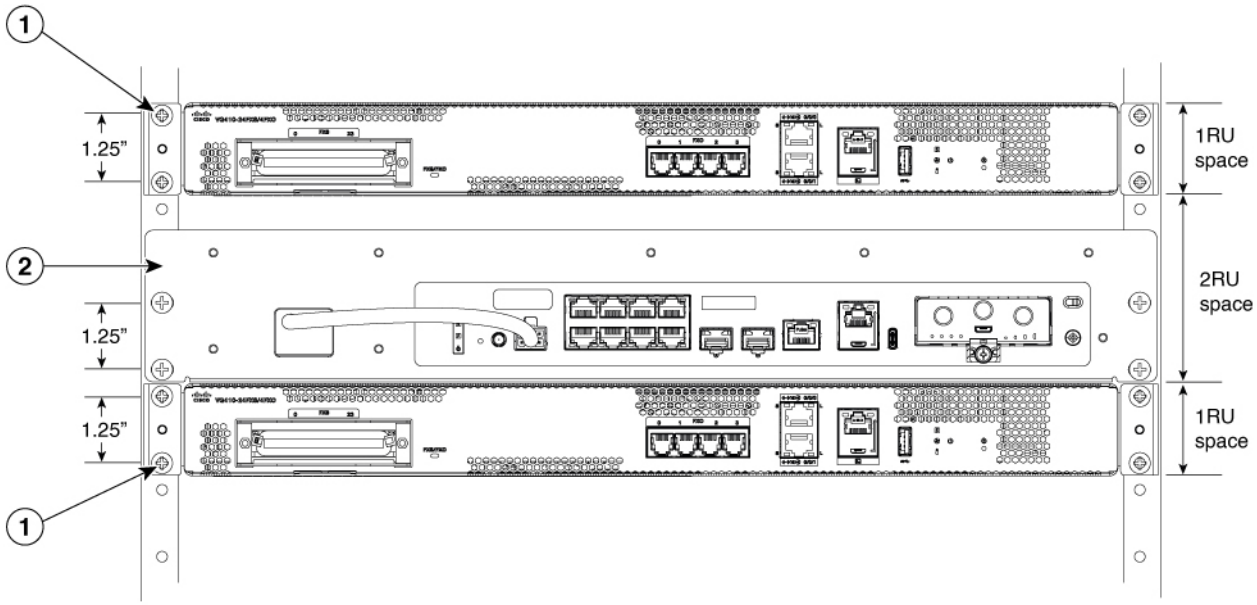


1	Ground location at back of the tray

Step 12 Install the rack-tray assembly into the rack by aligning the bottom of the rack-tray to the bottom of the Equipment Racks Rack-Unit (RU) spacing and secure the screws.

Note
The C8235-G2 Rack-tray is shorter than 2RU tall, but must be allocated the full 2RU of space.

Figure 33: Rack-tray assembly



1	Typical 1RU product (reference only)
2	C8235-G2 Rack-tray installed

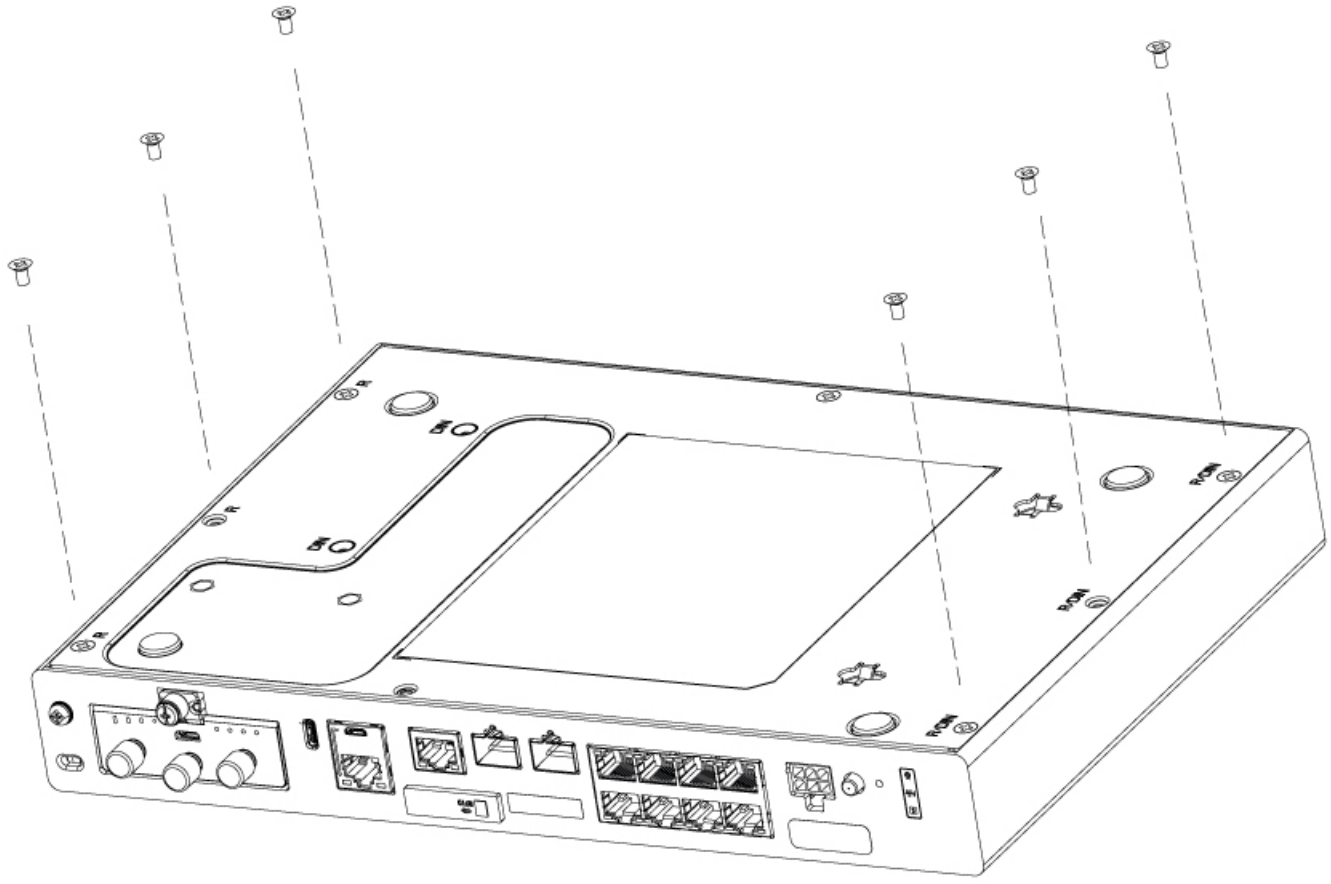
Mount the Router under a Desk or a Shelf

Installing the router under a desk requires an optional bracket kit that is not included with the router. The kit contains the rack-mount brackets and screws to secure the brackets the underside of a wooden desk or shelf. You can order these kits from your Cisco representative. This procedure describes how to mount a router under a desk or a shelf .

Procedure

Step 1 Remove qty (6) screws from the bottom side of the router. Keep the screws as they will be used later.

Figure 34: Remove the outer screws from the Router (C8235-G2 shown)



Step 2 Align one side of the bracket to the base and secure with 3 of the the flat-head screws that was removed. Follow the same steps to attach the second bracket to the opposite side.

Figure 35: Attaching Brackets to the Router

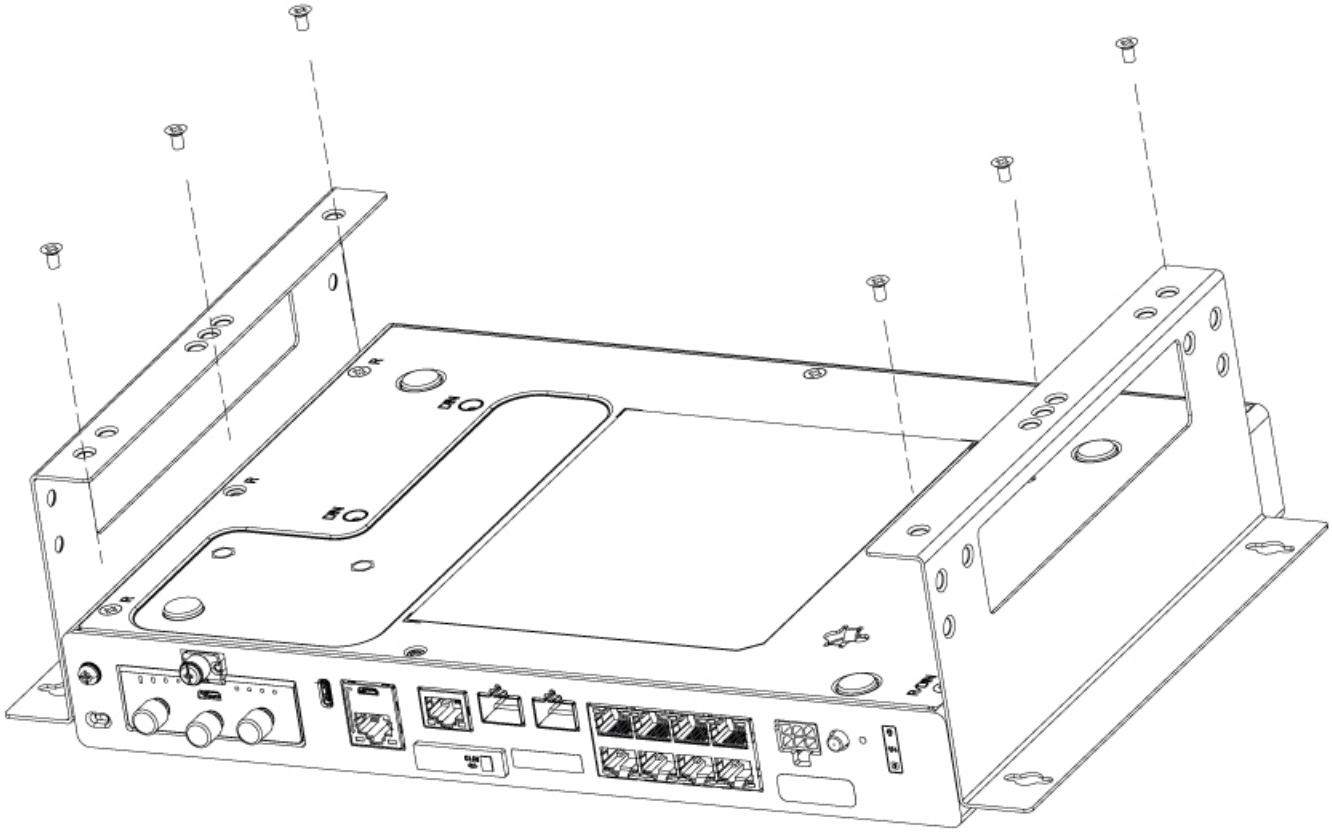
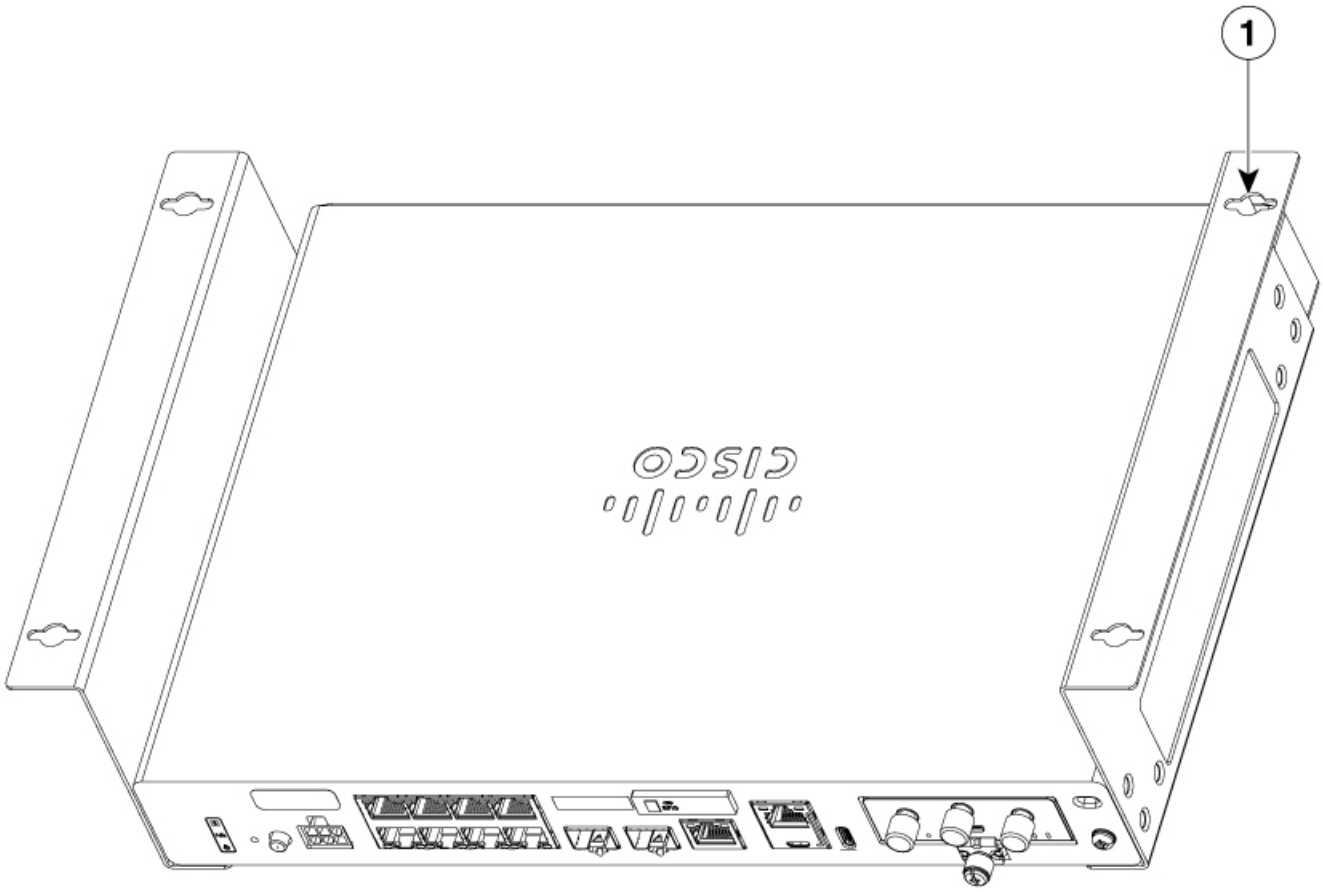


Figure 36: Router with the Brackets Attached (C8235-G2 shown)



Step 3 The router with the brackets attached can be used as a template to mark the screw locations to drill the pilot holes.

Figure 37: Mounting hole pattern for C8231-G2

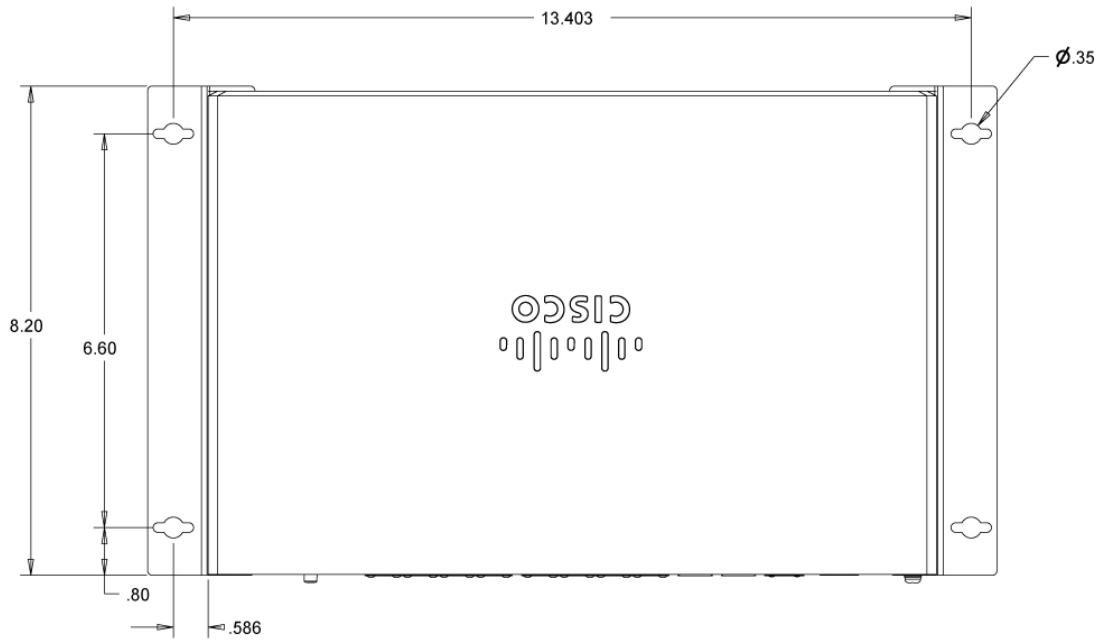
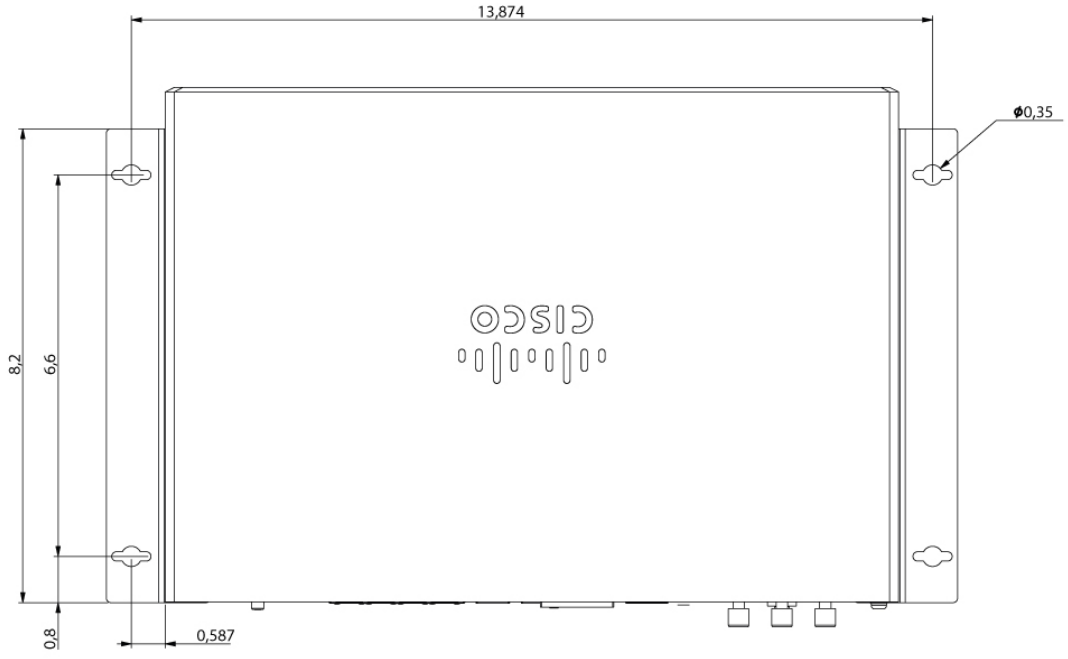


Figure 38: Mounting hole pattern for C8235-G2

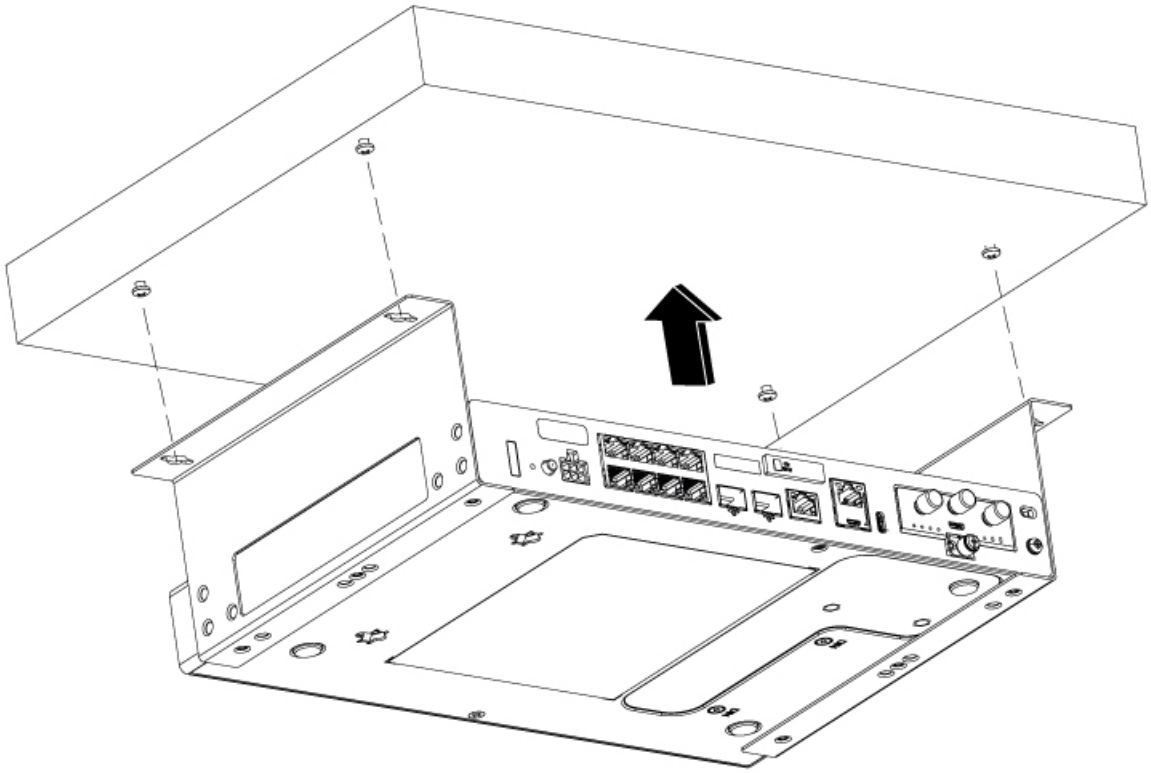


Note
Screws provided are size #8. It is recommended to drill a 1/8” pilot hole before installing the screws.

Step 4 Install the screws to the under the desk surface. Ensure to leave a gap between the screw-head and the desk surface. Align the large holes of each key-slot to each screw and push the router towards the desk.

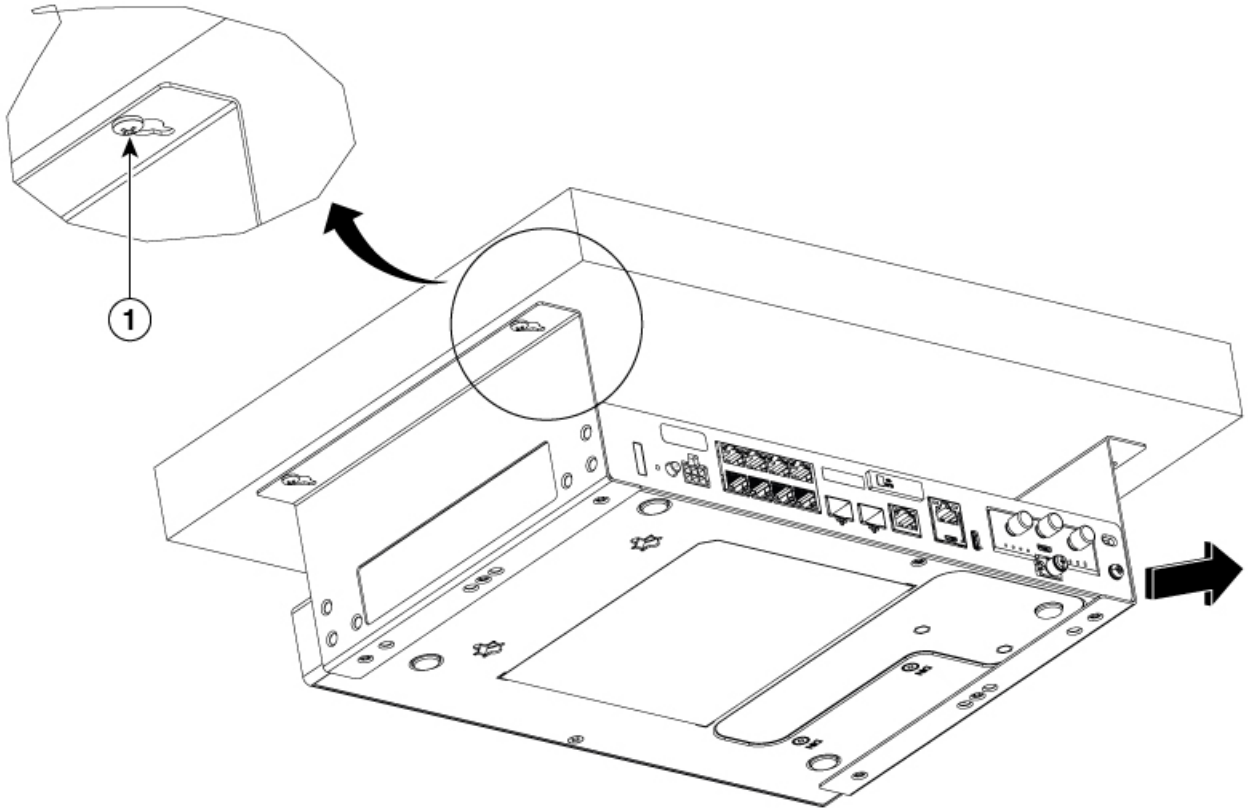
Figure 39: Pan-head Wood Screws

Figure 40: Mounting the Router under a Desk or Shelf



Step 5 When the bracket holes are past the screw heads, slide the assembly left or right to the thinner section of the key slot. Tighten the screws to secure the brackets.

Figure 41: Router mounted under the desk



Mount Router using DIN-Rail Brackets

Installing the router on a DIN-Rail requires an optional bracket kit not included with the router. Your chassis installation must allow unrestricted airflow for chassis cooling.

Attach Din-Rail Bracket on C8231-G2

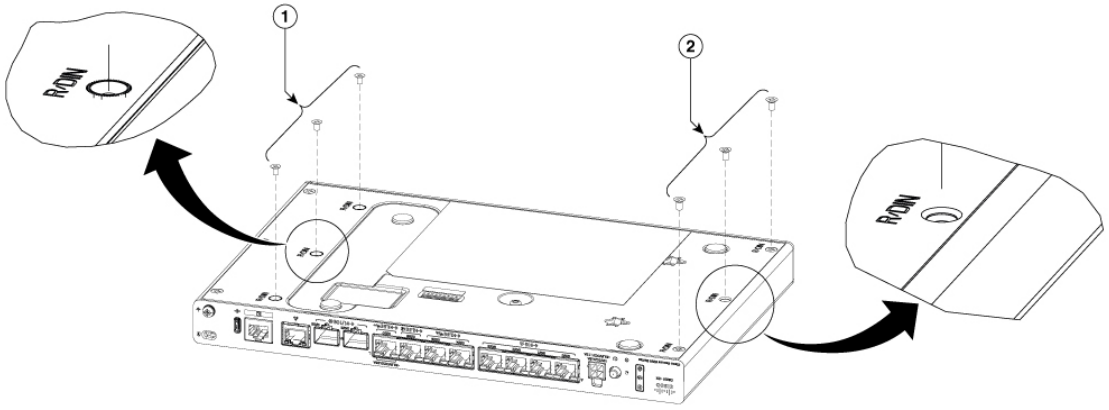
This procedure describes how to attach the bracket on the C8231-G2 router chassis:

Procedure

Step 1 Remove the six screws marked from the location with DIN from the bottom of the chassis.

Note
Three of the screws are black and need to be reassembled to the locations where they were removed.

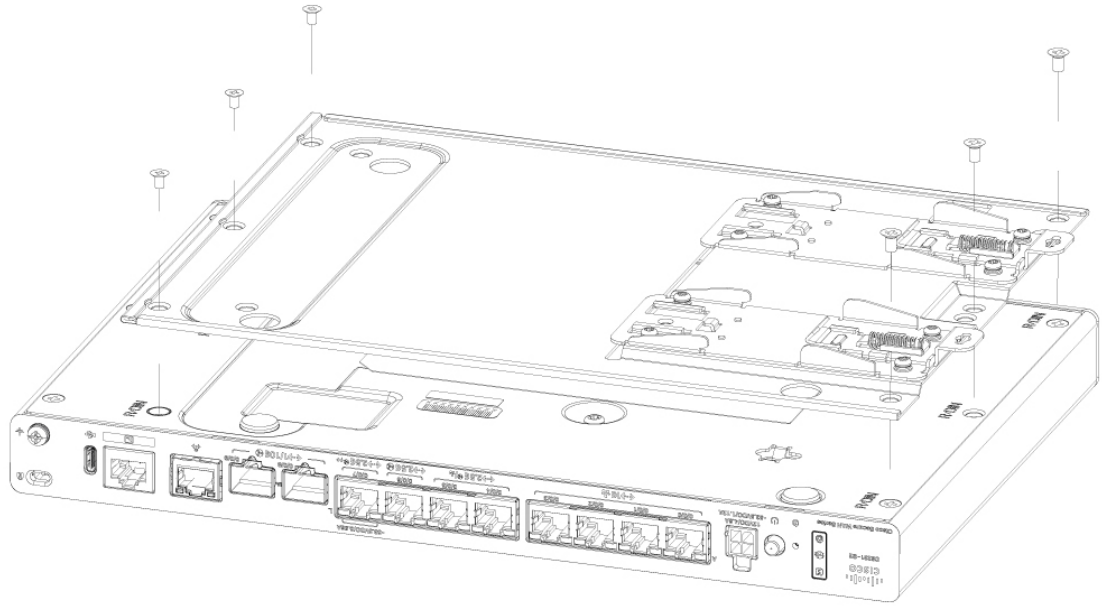
Figure 42: Attach the Din-Rail Brackets for C8231-G2



1	Router screws on the base of the router (black, M3)
2	Router screws on the base of the router (silver, #6-32)

Step 2 Place the din-rail bracket on the chassis and position the bracket over the six mounting holes. Secure the bracket by inserting the screws through the bracket. Ensure the black screws are secured in the same location.

Figure 43: Secure the Din-Rail Brackets for C8231-G2



Step 3 Once the bracket is attached to the router, it can be mounted onto the DIN rail.

Attach Din-Rail Bracket on C8235-G2

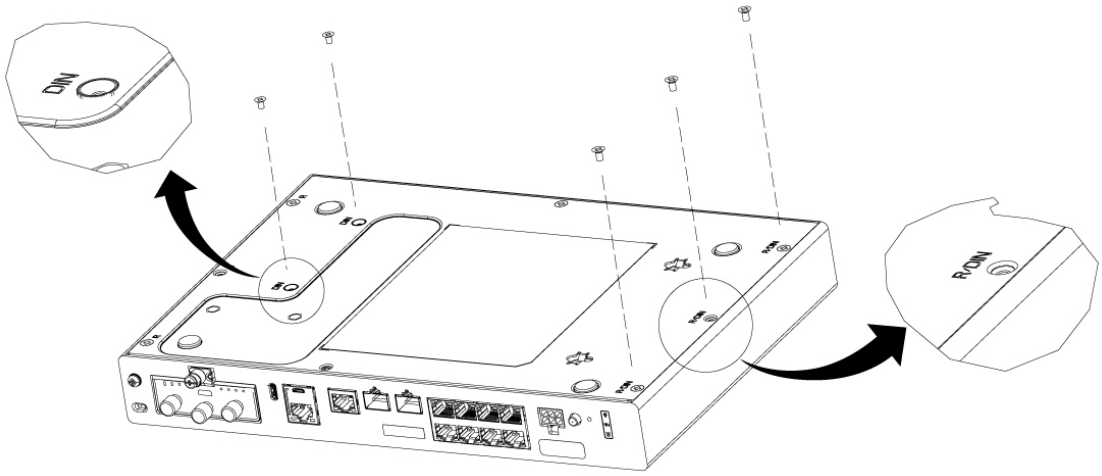
This procedure describes how to attach the bracket on the C8235-G2 router chassis:

Procedure

Step 1 Remove the five screws from location marked with DIN from the bottom of the chassis.

Example:

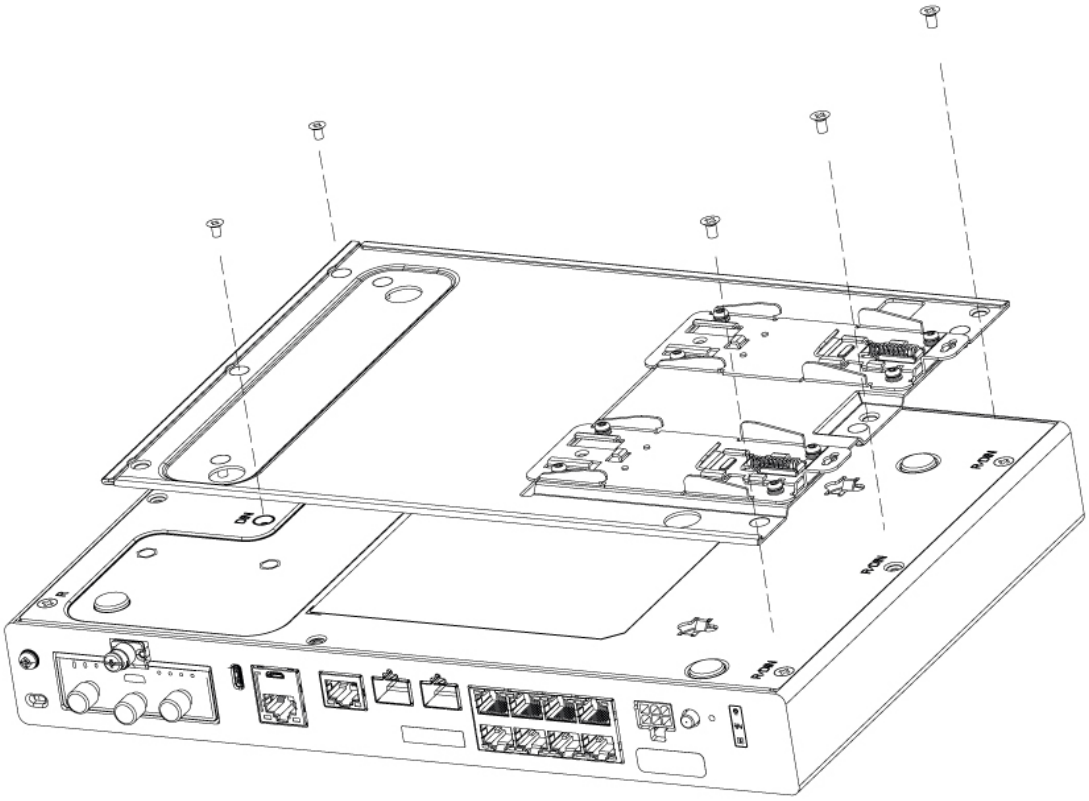
Figure 44: Attach the Din-Rail Brackets for C8235-G2



Step 2 Place the din-rail bracket on the chassis and position the bracket over the five mounting holes. Secure the bracket by inserting the screws through the bracket.

Example:

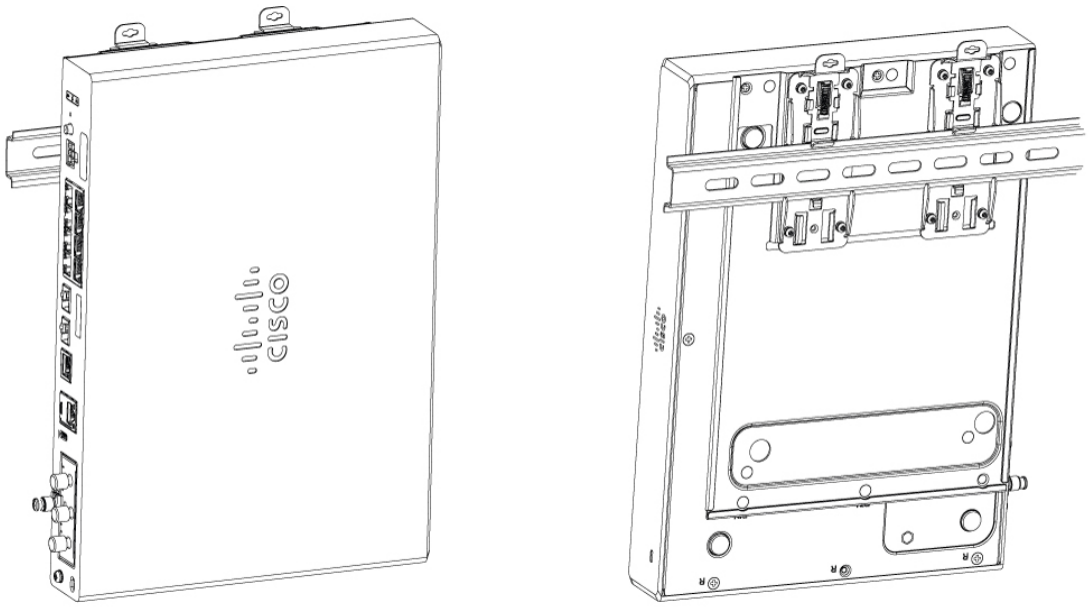
Figure 45: Secure the Din-Rail Brackets for C8235-G2



Step 3 Once the bracket is attached to the router, it can be mounted onto the DIN rail.

Example:

Figure 46: Mount the router using the DIN rail



Wall Mount the Router

The Cisco 8200 Series Secure Routers can be mounted using the Key-hole slots on the chassis base.

Warning **Statement 1094—**Read Wall-Mounting Instructions Before Installation

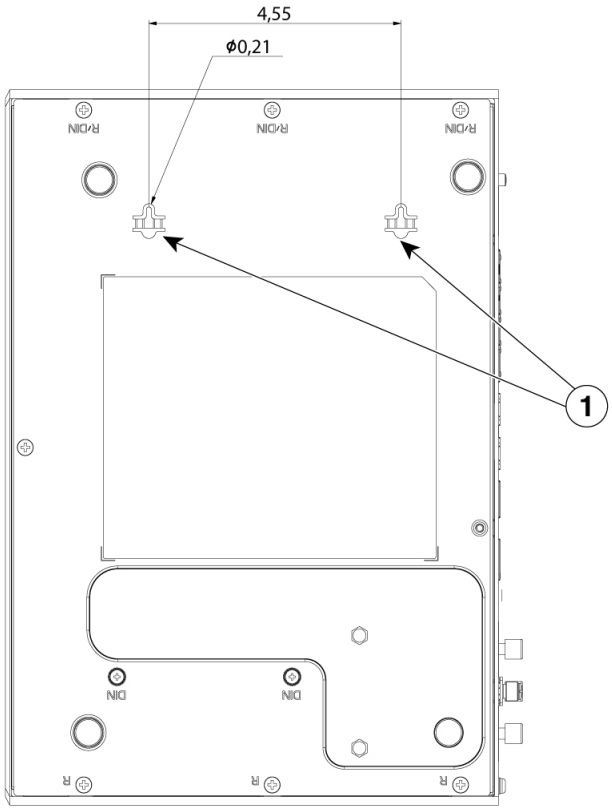
Read the wall-mounting instructions carefully before beginning installation. Failure to use the correct hardware or to follow the correct procedures could result in a hazardous situation to people and damage to the system.

Wall Mount Using Key-hole Slots

The Cisco 8200 Series Secure Routers have key-hole slots at the bottom of the chassis for mounting on a wall or other vertical surface.

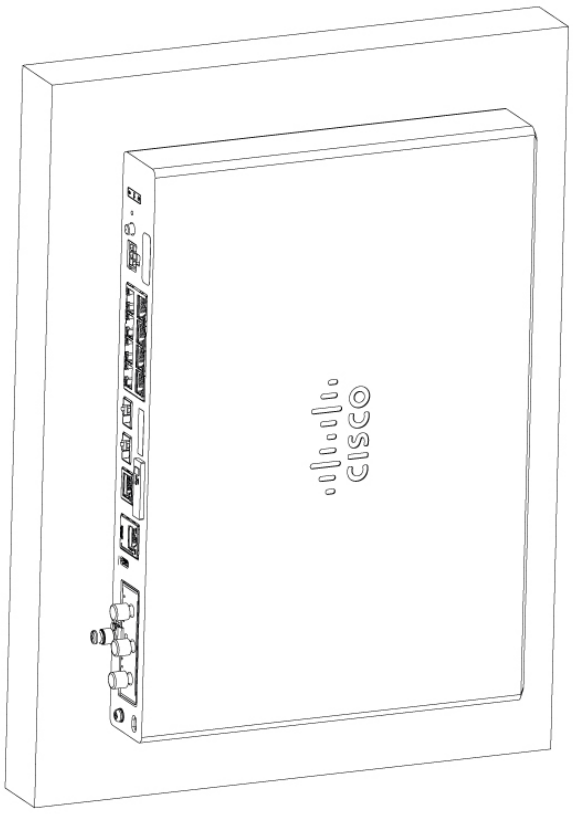
Note When choosing a location for wall mounting the router, consider cable limitations and wall structure.

Figure 47: Wall Mount Using Key-hole Slots - C8235-G2



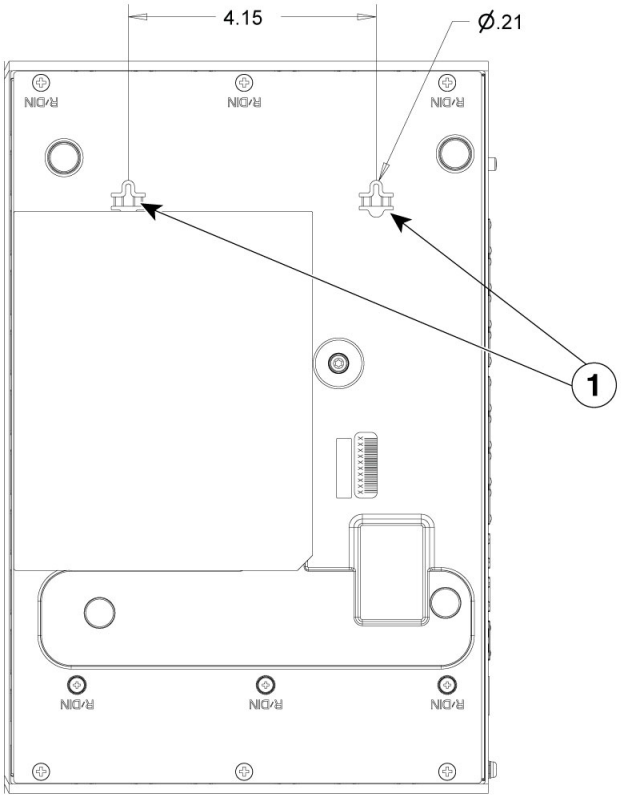
1	Key-hole slots

Figure 48: Wall Mount Orientation



1	Key-hole slots

Figure 49: Wall Mount Using Key-hole Slots - C8231-G2



1	Key-hole slots

Chassis Grounding

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

After you set up the router, connect the chassis to a reliable earth ground. The ground wire must be installed in accordance with local electrical safety standards. For safety information on grounding the chassis, refer to the chassis ground connection procedures.

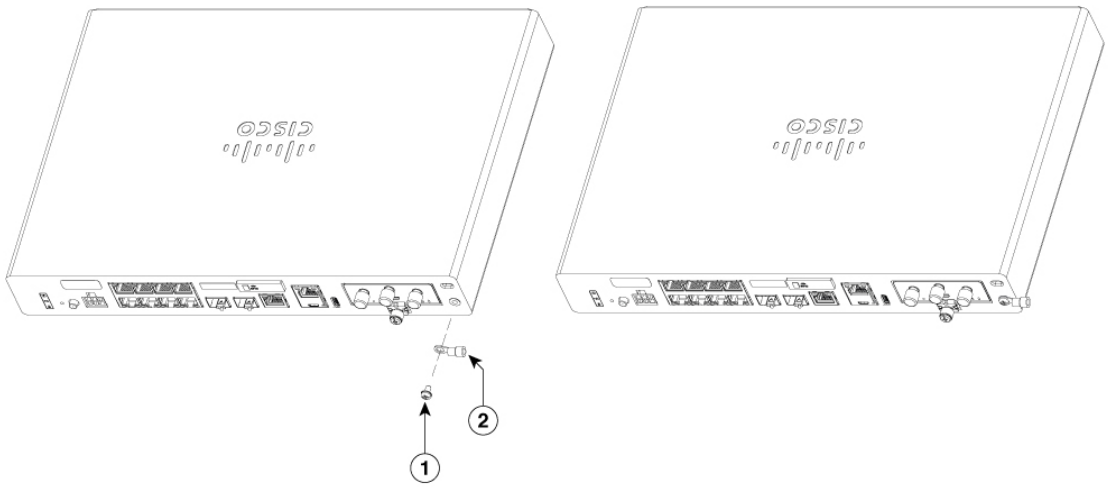
1. For grounding the chassis, use a copper wire of size of 14 AWG (2 mm²) and a ground lug. These are not provided with the router.
2. Use the UNC 6-32 screw, which has a length of about 0.25 inches.

To install the ground connection for your router, perform these steps:

1. Strip one end of the ground wire to the length required for the ground lug or terminal.
2. Crimp the ground wire to the ground lug or ring terminal, using a crimp tool of the appropriate size.

3. Attach the ground lug or ring terminal to the chassis as shown in the figures using the screw for the ground lug on the front of the router. Tighten the screw; the recommended torque is 8 to 10 inch-lbf (0.9 to 1.1 N-m).

Figure 50: Chassis Ground Connection Cisco 8200 Series Secure Routers

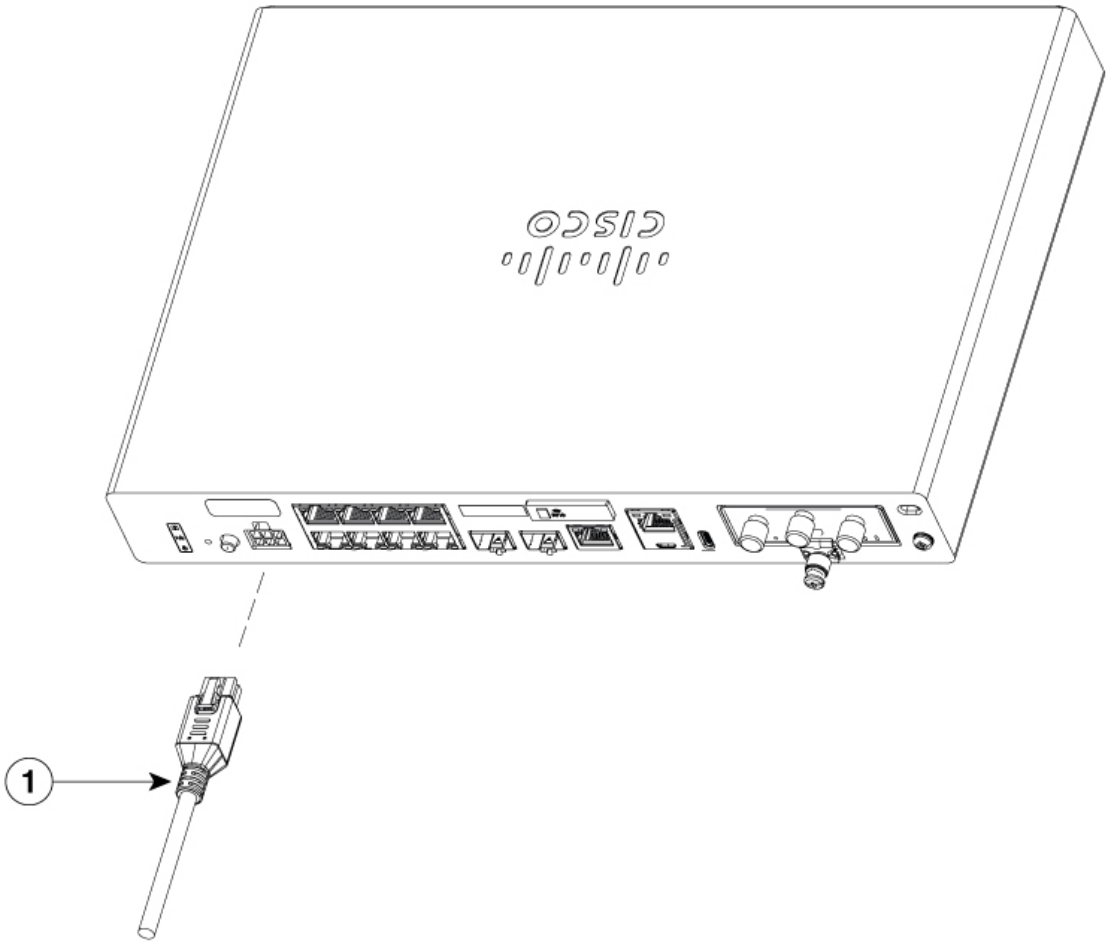


1	Screw (UNC 6-32)
2	Ground Lug (Customer provided)

Connect Power Cable

Power supply of the Cisco 8200 Series Secure Routers is an external AC to DC power adapter. The external DC power connector plugs into the router's 4 points power connector.

Figure 51: Power Cable for Cisco 8200 Series Secure Routers



1.	Power Cable

Install the Silicon Labs USB Device Driver

This section contains the following 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)** dropdown.

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 values for the **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.

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 **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 shows response upon first **Enter** key if there is no output.

Connect WAN and LAN Interfaces

This section describes how to connect WAN and LAN interface cables. Before you connect the interface cables, refer to the following warning statements:

Ports and Cabling

This section summarizes typical WAN and LAN connections for Cisco 8200 Series Secure Routers. The connections summarized here are described in detail in the Cisco Modular Access Router Cable Specifications document on cisco.com.

Table 6: WAN and LAN Connections

Port or Connection	Port Type, Color[1]	Connection	Cable
Ethernet	RJ-45	Ethernet hub or Ethernet switch	Category 5 or higher Ethernet
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

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

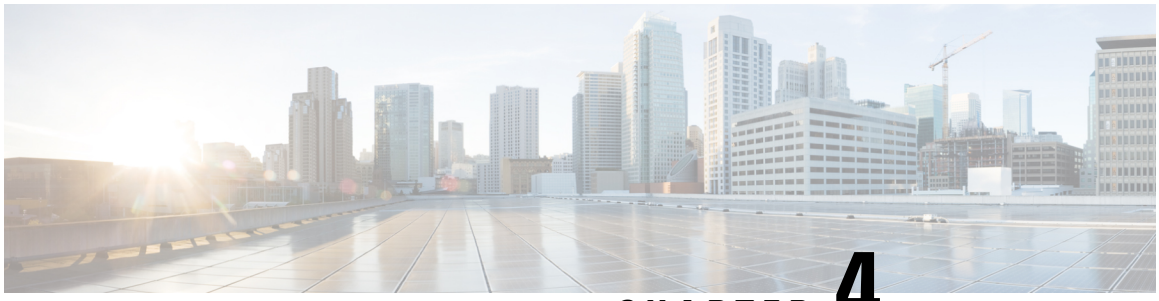
Connection Procedures and Precautions

After you have installed the router chassis, perform these steps to connect the WAN and LAN interfaces:

- Connect each WAN and LAN to the appropriate connector on the chassis.
- Position the cables carefully so that you do not strain 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. If necessary, reposition the cables.
- Install cable ties in accordance with site requirements.

Configure the Router at Startup

After installing the router and connecting the cables, you can configure the router with basic configurations. For more information on how to configure the router, see the Cisco 8200 Series Secure Software Configuration Guide.



CHAPTER 4

Install and Upgrade Field Replaceable Units

The Cisco 8200 Series Secure Routers have field-replaceable units (FRUs) that can be quickly and easily removed and replaced without having to send the entire router for repair.

This chapter describes how to install FRUs in the Cisco 8200 Series Secure Routers. The information is contained in the following sections:

External Modules

This section describes how to install external modules and FRUs in the Cisco 8200 Series Secure Routers. The information is contained in the following sections:

Install and Remove Small Form Pluggable Modules

This section describes how to install and remove Small Form Pluggable (SFP) modules in the Cisco 8200 Series Secure Routers.

Only SFP modules certified by Cisco and complies with IEC 60825-1:2014 are supported on these routers. For more information, refer to SFPs Supported on Cisco 8200 Series Secure Routers.

Take note of the following optical connection warnings:

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 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.

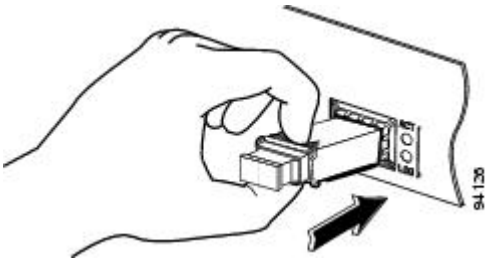
Install SFP Modules

To install a SFP module in your router:

1. Disconnect the power supply before you replace any module.
2. Slide the SFP into the router connector until it locks into position.

Note The following image is for reference only.

Figure 52: Install an SFP Module



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

3. Connect the network cable to the SFP module.

Remove SFP Modules

To remove a SFP module on your router:

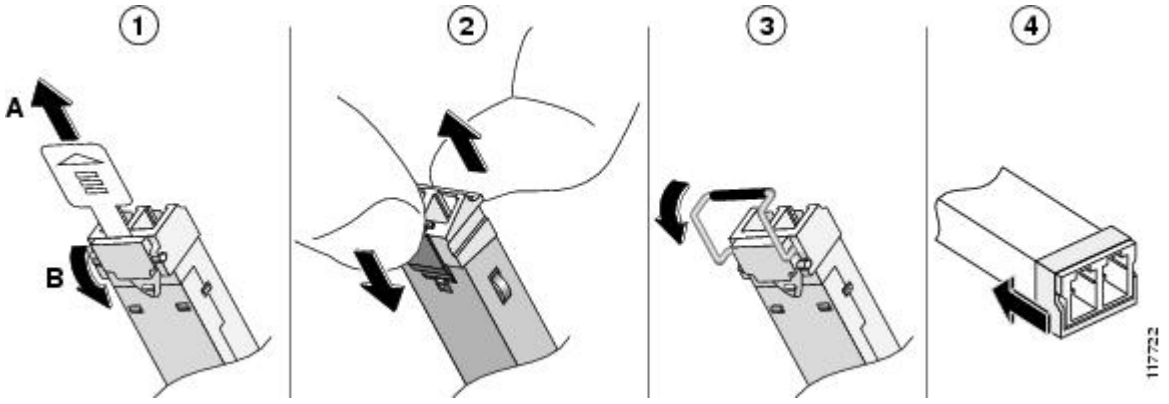
1. Disconnect the power supply and remove all cables from the SFP module.

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

2. 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 models or technology type. For information on the SFP technology type and model, see the label on the side of the SFP.

Figure 53: Latch Mechanisms for Disconnecting SFP Modules



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

3. Grasp the SFP on both sides and remove it from the router.

Install a Pluggable Interface Module

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 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.

Install a Pluggable Interface Module on a C8235-G2

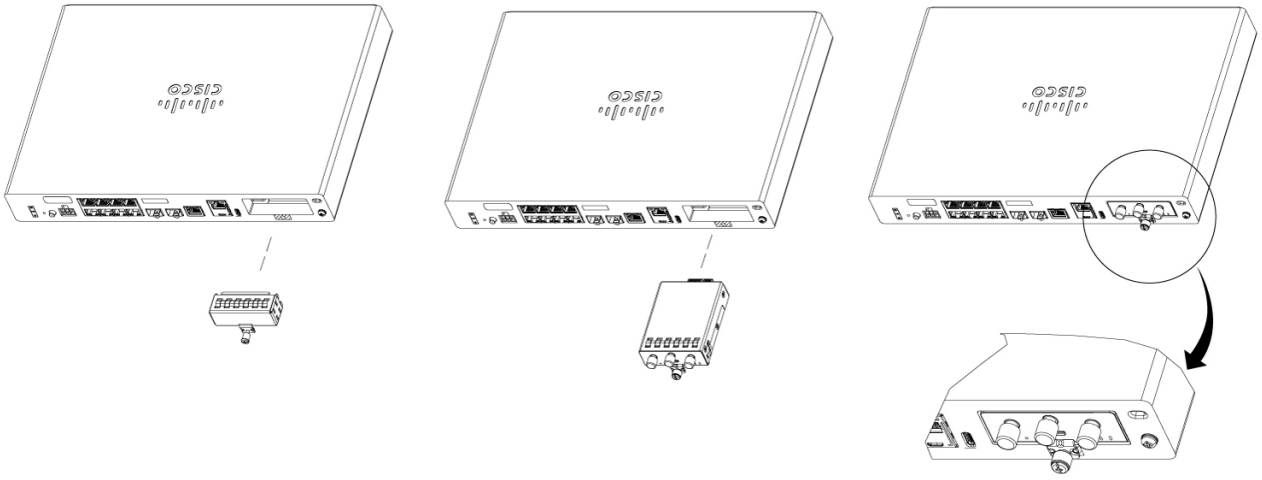
To insert the pluggable interface module into the router, follow these steps:

Procedure

Step 1 Insert and then gently push the LTE pluggable into the pluggable slot of C8235-G2 until firmly fixed.

Step 2 Tighten the screw, the recommended torque is 10-12 in-lb.

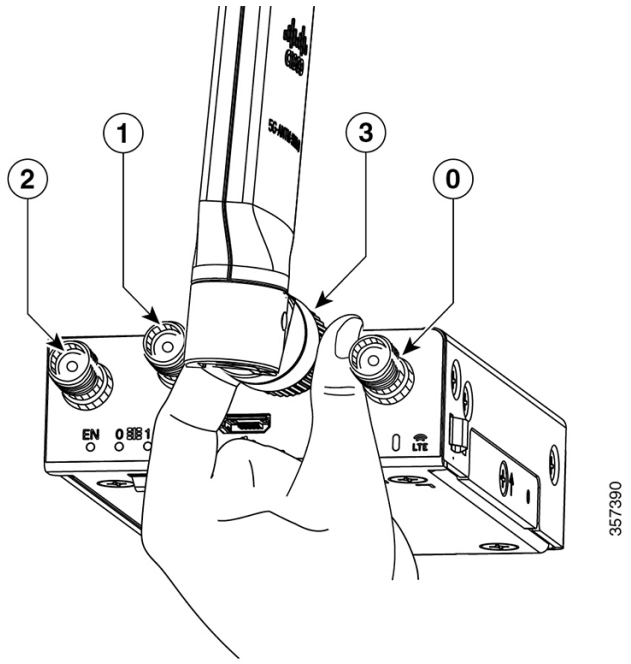
Figure 54: LTE Pluggable Interface Module - C8235-G2



Configuring a Pluggable Interface Module

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

Figure 55: Attaching the Antennas



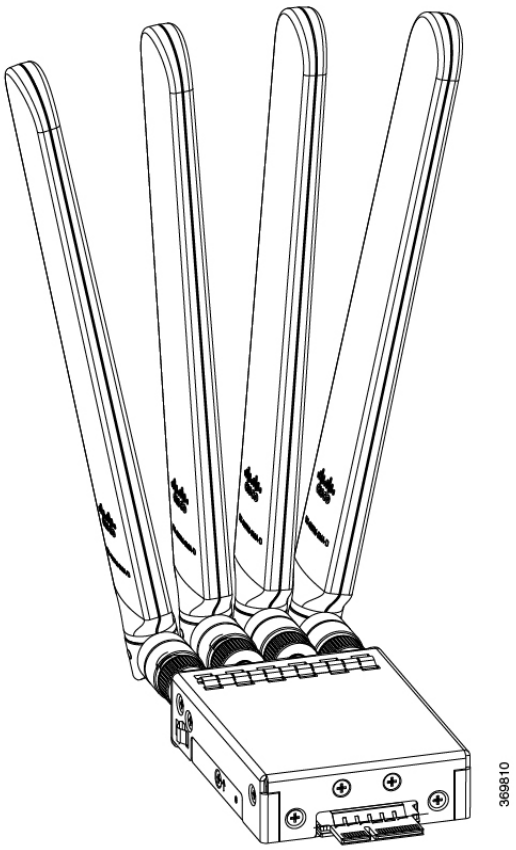
Procedure

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 because it helps in getting higher RF performance.



RF Band Mapping for Antenna Ports (For P-5GS6-R16SA-GL)

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

RF Band Mapping for Antenna Ports for P-5GS6-R16SA-GL

Radio Access Technology (RAT)	Bands	Tx Antennas		Rx Antennas				GNSS Antenna
		Default	Alternate Path	ANT0	ANT1	ANT2	ANT3	GPS

Radio Access Technology (RAT)	Bands	Tx Antennas		Rx Antennas				GNSS Antenna
5GNR Sub-6G	29	-	-	Y	-	Y	-	-
	38, 41	ANT2	ANT0	Y	Y	Y	Y	-
	48	ANT3	ANT1	Y	Y	Y	Y	-
	75, 76	-	-	Y	Y	Y	Y	-
	77, 78	ANT3	ANT1 ANT2	Y	Y	Y	Y	-
	79	ANT3	ANT1	Y	Y	Y	Y	-
LB LTE/ 5GNR Sub-6G	5, 8, 12, 13, 14, 17, 18, 19, 20, 26, 28, 71	ANT0	-	Y	-	Y	-	-
MB/HB LTE/ 5G NR Sub-6G	1, 2, 3, 4, 7, 25, 30, 39, 40, 66, 70	ANT0	-	Y	Y	Y	Y	-
LTE	29	-	-	Y	-	-	Y	-
	34	ANT0	-	Y	-	Y	-	-
	46	-	-	Y	-	-	Y	-
	32	-	-	Y	Y	Y	Y	-
	38	ANT0	-	Y	Y	Y	Y	-
	41	ANT0	ANT2	Y	Y	Y	Y	-
	42, 43, 48	ANT3	ANT1	Y	Y	Y	Y	-
WCDMA	1, 2, 4, 5, 8, 19	ANT0	-	Y	-	Y	-	-
GNSS	-	-	-	-	-	-	-	L1

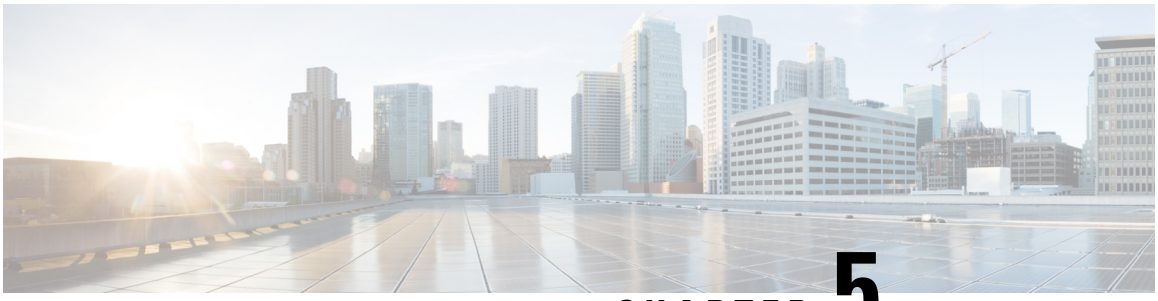
LED Behaviors

The following table lists the LED indicators and their behavior. The LEDs provide a visual indication of the status and the currently selected services.

LED Indicators:

LED	Color	Function
EN	Green, Yellow	**Enable LED** • Pluggable enable LED • Off: System power is off • Yellow: Module power is not functioning correctly • Green: Module power is on
SIM0	Green, Yellow	**SIM0 LED/Activity** • SIM0 LED status and WWAN activity • Off: SIM0 is not installed • Yellow: SIM0 is installed, but not active • Green: SIM0 installed and active • Green Blink: LTE data activity
SIM1	Green, Yellow	**SIM1 LED/Activity** • SIM1 LED status and WWAN activity • Off: SIM1 is not installed • Yellow: SIM1 is installed, but not active • Green: SIM1 installed and active • Green Blink: LTE data activity
GPS	Green, Yellow	**GPS LED** • Off: GPS is not configured • Yellow: Software is defined • Green: GPS is configured • Green Blink: GPS is functional
RSSI	Green, Yellow	**RSSI LED (Applicable for P-LTE-XX, P-LTEA-XX, P-LTEAP18-GL)** • Green: 4G LTE

LED	Color	Function
		• Yellow: 3G



CHAPTER 5

ROM Monitor Overview

The *ROM Monitor software* is also known as *ROMMON*, *boot software*, *boot image*, or *boot helper*. Although it is distributed with routers that use the Cisco IOS XE software, the ROMMON is a separate program from the Cisco IOS XE software. During normal startup, ROMMON initializes the router, and then, the control passes to the Cisco IOS XE software.

When you connect a terminal to the router that is in ROMMON mode, the ROMMON command-line interface (CLI) prompt is displayed.

Access the ROMMON mode to perform these tasks:

- Specify config-register value to use for the next boot up
- Boot a valid IOS XE image
- Bypass NVRAM settings and config-register value for password recovery

Note After the Cisco IOS XE software boots up, ROMMON is no longer in use.

Environmental Variables and the Configuration Register

Two primary connections exist between ROMMON and the Cisco IOS XE software: the ROMMON environment variables and the configuration register.

The ROMMON environment variables define the location of the Cisco IOS XE software and describe how to load it. After ROMMON has initialized the router, it uses the environment variables to locate and load the Cisco IOS XE software.

The *configuration register* is a software setting that controls how a router starts up. One of the primary uses of the configuration register setting is to control whether the router starts in ROMMON mode or Administration EXEC mode. The configuration register is set in either ROMMON mode or Administration EXEC mode as needed. You can set the configuration register using the Cisco IOS XE software prompt when you need to use ROMMON mode. When maintenance in ROMMODE mode is complete, change the configuration register back so that the router reboots with the Cisco IOS XE software.

Access ROMMON Mode with a Terminal Connection

When the router is in ROMMODE mode, you can access the ROMMODE software only from a terminal connected directly to the console port of the card. Because the Cisco IOS XE software (EXEC mode) is in

operatiion, the nonmanagement interfaces are not accessible. Therefore, all Cisco IOS XE software resources are unavailable.

Network Management Access and ROMMON Mode

ROMMON mode is a router mode, not a mode within the Cisco IOS XE software. The ROMMON software and the Cisco IOS XE software are two separate programs that run on the same router. At any given time, the router is running one of these programs, but it never runs both at the same time.

One area that can be confusing when using ROMMON and the Cisco IOS XE software is the area that defines the IP configuration for the Management Ethernet interface. Most users are comfortable with configuring the Management Ethernet interface in the Cisco IOS XE software. When the router is in ROMMON mode, however, the router is not running the Cisco IOS XE software, therefore, Management Ethernet interface configuration is not available.

When you want to access other devices, such as a TFTP server, while in ROMMON mode on the router, you must configure the ROMMON variables with IP access information.

For more information on ROMMON and Basic Procedures, refer to the Upgrading Field-Programmable Hardware Devices for Cisco 8200 Series Secure Routers.

INDEX