



# Cisco 12006 and Cisco 12406 Router Blower Module and Air Filter Replacement Instructions

---

**Product Number:** GSR6-BLOWER=, 12000/6-BLOWER=, ACS-GSR6-FLTR=

This guide contains removal and replacement procedures for blower module and air filters in a Cisco 12006 or Cisco 12406 Router. Unless otherwise noted, all information in this publication applies to both router models.



## Note

The illustrations in this guide represent both the original and newer enhanced capacity blower modules, and air filters for the Cisco 12006 or Cisco 12406 router. Depending on your system, these components may not look *exactly* like those in your chassis, but the removal and replacement procedures are essentially the same. For clarity, most chassis covers are not shown in the illustrations.

---

## Contents

- [Blower Module Compatibility, page 2](#)
- [Prerequisites and Preparation, page 2](#)
- [Installation Guidelines, page 4](#)
- [Removing and Replacing the Blower Module, page 5](#)
- [Troubleshooting the Installation, page 7](#)
- [Cleaning or Replacing the Air Filters, page 8](#)
- [Regulatory, Compliance, and Safety Information, page 9](#)
- [Obtaining Documentation, page 11](#)
- [Documentation Feedback, page 12](#)
- [Cisco Product Security Overview, page 13](#)
- [Obtaining Technical Assistance, page 14](#)
- [Obtaining Additional Publications and Information, page 15](#)



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

Copyright © 2005 Cisco Systems, Inc. All rights reserved.

# Blower Module Compatibility

Two types of blower modules are used for the Cisco 12006 and Cisco 12406 routers; blowers that shipped with original systems, and enhanced capacity blowers that ship with current systems. If you are replacing an:

- Original blower module (GSR6-BLOWER=)—Use an original blower module *or* an enhanced capacity blower module as a replacement.
- Enhanced capacity blower module (12000/6-BLOWER=)—Use an enhanced capacity blower module as a replacement.



## Note

Compared to the original blower modules that shipped with Cisco 12006 and Cisco 12406 routers, airflow capacity for new enhanced blower modules is increased by nearly 40 percent to provide additional cooling to the chassis. The new fans operate at a higher speed to provide improved airflow, so you may notice increased sound generated from the new blower module.

## Prerequisites and Preparation

Before you perform any of the procedures in this guide, we recommend:

- Read the safety and ESD-prevention guidelines in this section.
- Ensure that you have all of the necessary tools and equipment before beginning the installation (see the [“Installation Guidelines” section on page 4](#)).
- Have access to the following documents during the installation:
  - *Regulatory Compliance and Safety Information for the Cisco 12000 Series Router* publication that shipped with the router (78-4347-xx)
  - *Cisco 12006 and Cisco 12406 Router Installation and Configuration Guide*

For additional information about obtaining documentation see the [“Obtaining Documentation” section on page 11](#).

## Safety Guidelines

Before you perform any procedure in this publication, review the safety guidelines in this section to avoid injuring yourself or damaging the equipment.

## Safety Warnings

Safety warnings appear throughout this publication in procedures that, if performed incorrectly, may harm you. A warning symbol precedes each warning statement. The following warning is an example of a safety warning. It identifies the warning symbol and associates it with a bodily injury hazard.



This warning symbol means danger. You are in a situation that could cause bodily injury. Before you work on any equipment, be aware of the hazards involved with electrical circuitry and be familiar with standard practices for preventing accidents. To see translations of the warnings that appear in this publication, refer to the Regulatory Compliance and Safety Information document that accompanied this device.

## Preventing Electrostatic Discharge Damage

Many router components can be damaged by static electricity. Not exercising the proper electrostatic discharge (ESD) precautions can result in intermittent or complete component failures. To minimize the potential for ESD damage, always use an ESD-preventive antistatic wrist strap (or ankle strap) and ensure that it makes good skin contact.

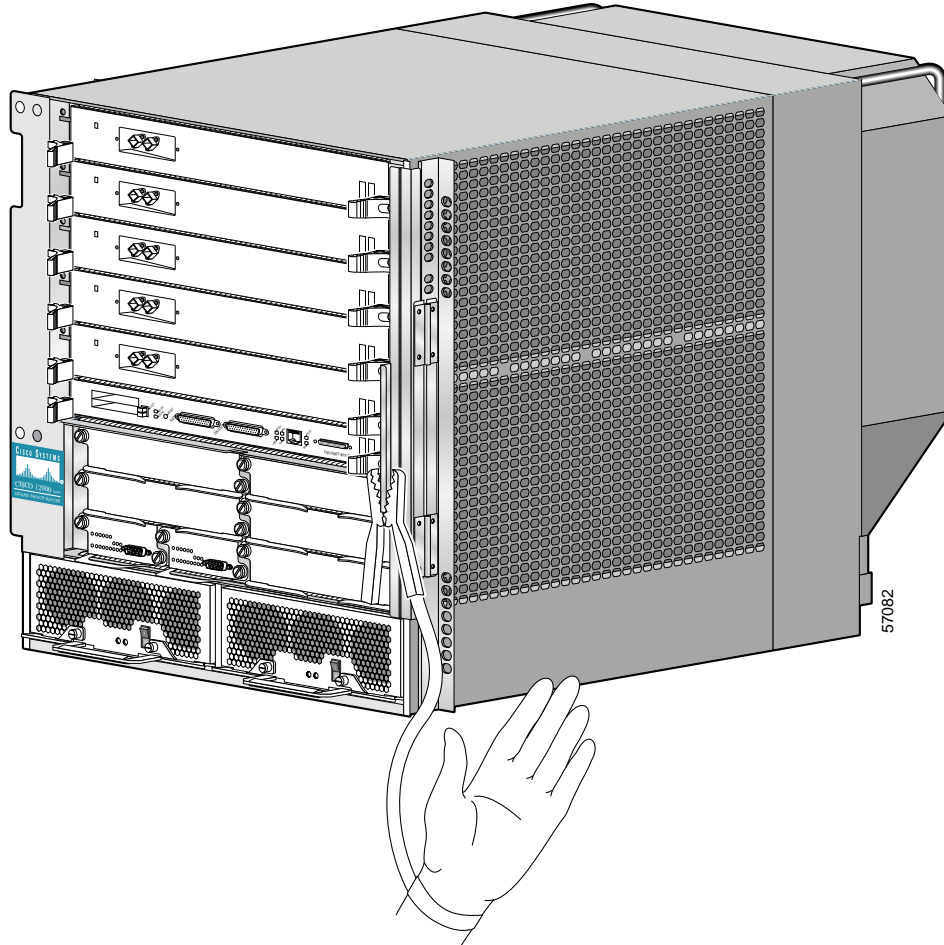


### Note

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

Before performing the procedures in this guide, attach an ESD-preventive strap to your wrist and connect the leash to the chassis or to another grounded, bare metal surface as shown in [Figure 1](#).

**Figure 1** Connecting an ESD-preventive Wrist Strap to the Chassis



## Installation Guidelines

The blower module supports online insertion and removal (OIR), so you can remove and install the blower module while the system remains powered on without presenting an electrical hazard or damage to the system. This feature lets you replace the blower module while the system maintains all routing information and ensures session preservation.



**Caution**

Although the blower module supports OIR and can be replaced without interruption to system operation, do not operate the system without the blower module for more than a few minutes to prevent overheating.

## Required Tools and Equipment

You need the following tools and equipment to install the blower module:

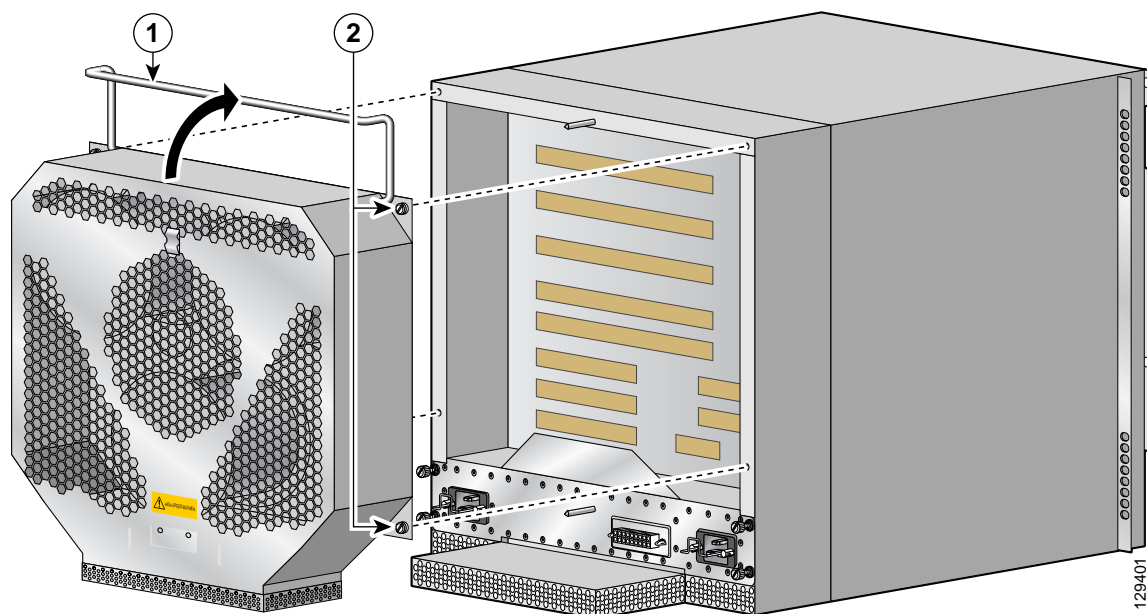
- Number 2 Phillips screwdriver
- 3/16-inch flat-blade screwdriver
- An electrostatic discharge (ESD) preventive wrist or ankle strap with connection cord
- Vacuum cleaner (to clean the air filters)

## Removing and Replacing the Blower Module

Use the following procedure to remove and replace the blower module.

- Step 1** Remove the blower module from the chassis ([Figure 2](#)):
- a. Lift the blower module handle to its carrying position.
  - b. Loosen the four captive screws on the blower module faceplate.
  - c. Remove the blower module by grasping it on each side and pulling it straight back from the chassis.

**Figure 2** Removing the Blower Module



1 Carrying handle

2 Captive screws (2 on each side)

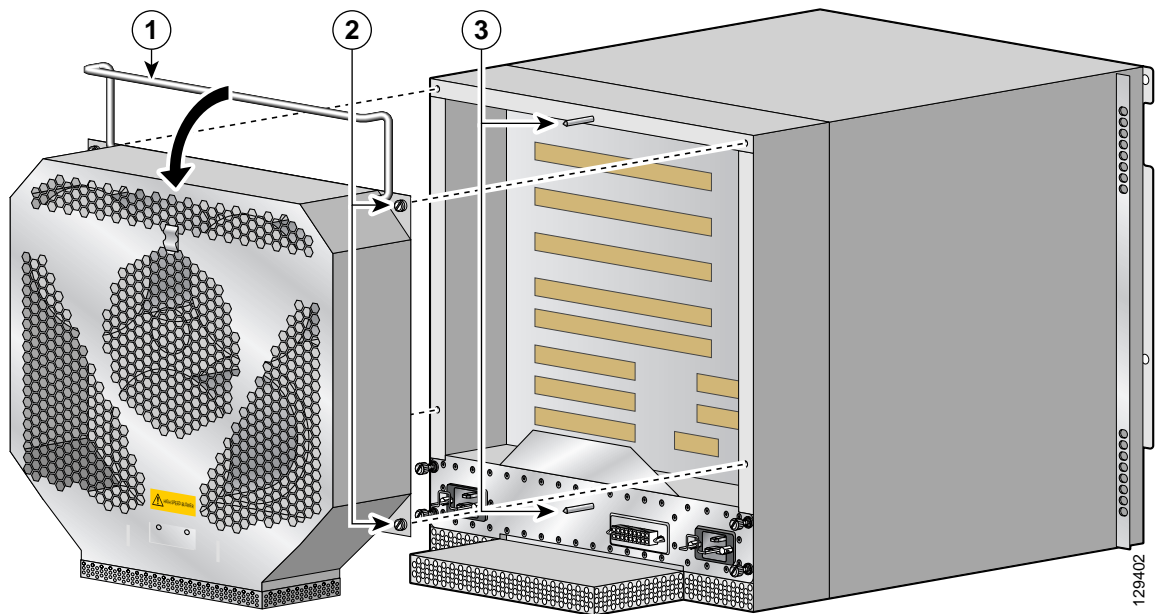
- Step 2** Install the new blower module ([Figure 3](#)):
- Position the alignment holes on the blower module with the guide pins at the top of the chassis and on the PDU at the bottom of the chassis.
  - Slide the blower toward the chassis until it mates with the backplane connector.



Electrical and control line connections for the blower module and backplane occur automatically when the connectors on the blower module and PDU mate. To prevent damage to the blower module and PDU connectors, do not use excessive force when installing the blower module against the rear of the chassis.

- Tighten the four captive screws to secure the blower module to the chassis.  
The (green) OK indicator should light. If the OK indicator does not light, see the [“Troubleshooting the Installation”](#) section on page 7.
- Lower the blower module handle to its operating position.

**Figure 3** *Installing the Blower Module*



1	Carrying handle	2	Captive screws (2 on each side)
3	Guide pins		

# Troubleshooting the Installation

Use the following procedure to troubleshoot the blower module if it is not operating properly after installation.

- 
- Step 1** Be sure the router is powered on and that all power cords are connected properly.
- Step 2** Loosen the four captive screws and reseal the blower module to the chassis. Retighten the captive screws to ensure the blower module is properly seated to the backplane connector.
- Step 3** Check the blower module status indicators:
- OK (green)—This indicator should light as soon as the blower module is installed and receives power from the backplane connector. It indicates that the blower module is operating normally.
  - Fail (red)—This indicator remains off during normal operation. If the indicator is on, the system has detected a fan failure or other fault in the blower module.
    - If this indicator remains on and the blower module fans fail to operate normally after several attempts to reseal the blower module, replace the existing blower module with a spare.
    - If the spare blower module also fails, power off the router and contact a Cisco service representative for assistance.
-

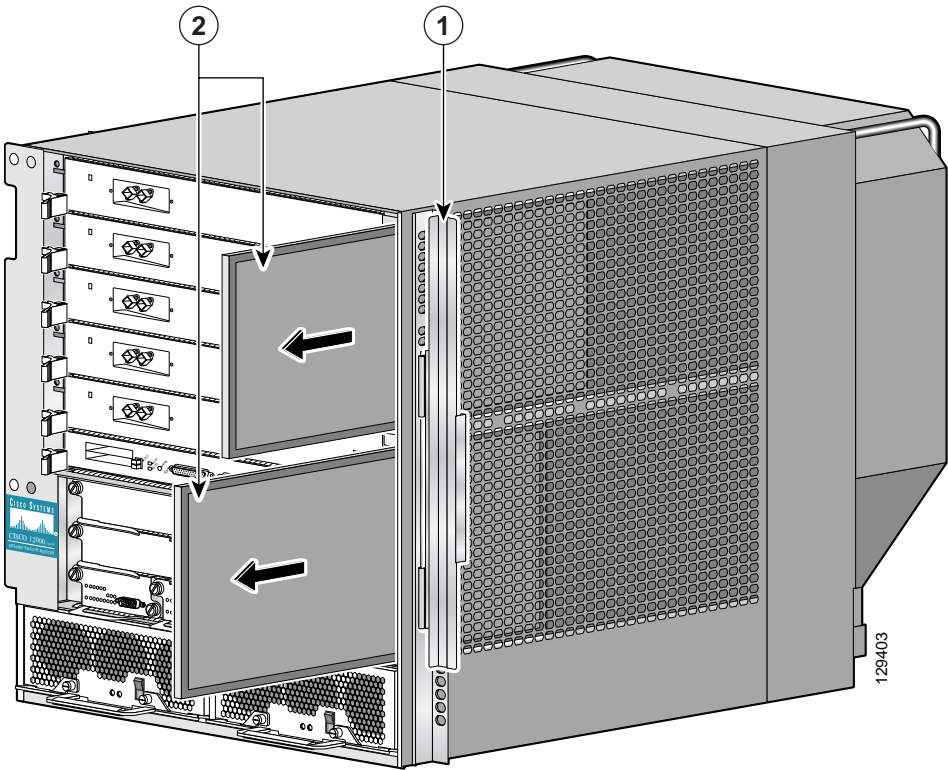
# Cleaning or Replacing the Air Filters

The Cisco 12006 and Cisco 12406 routers are equipped with two user-serviceable air filters that remove dust drawn into the router by the blower module. One time per month (or more often in dusty environments), examine the air filters.

Use the following procedure to clean or replace the air filters.

- Step 1
- Open the spring-loaded air filter door on the right side of the chassis and remove an air filter by pulling the small tab on the edge of the filter (Figure 4).  
Remove the second air filter the same way.

Figure 4 Removing the Air Filters



1	Air filter door	2	Air filters
---	-----------------	---	-------------



**Step 2** Visually check the condition of the air filters to determine whether to clean them or install new replacements.

- Dirty—You can vacuum or replace the filters.



**Caution**

Do not try to vacuum the air filter while it is installed in the chassis. You must remove the air filter completely before you clean it to prevent contaminants from being drawn into the router.

- Worn or torn—If the filters appear worn or torn, dispose of them in a responsible manner and install replacement air filters (ACS-GSR6-FLTR=).

**Step 3** Open the air filter door and install the new or cleaned air filters.



**Note**

An arrow located on the edge of each air filter frame that indicates the direction of *air flow*. Always install the air filter with the arrow pointing in toward the RP and line card cage.

## Regulatory, Compliance, and Safety Information

This section includes regulatory, compliance, and safety information.

### Translated Safety Warnings and Agency Approvals

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

### Electromagnetic Compatibility Regulatory Statements

#### FCC Class A Compliance

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

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

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

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

## CISPR 22

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

## Canada

### English Statement of Compliance

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

### French Statement of Compliance

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

## Europe—EU

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

## VCCI Class A Notice for Japan



### Warning

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

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

## Class A Notice for Hungary



Warning

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

Figyelem

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

## Class A Notice for Taiwan and Other Traditional Chinese Markets



Warning

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

警告

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

## Class A Notice for Korea



Warning

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

주의

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

## Obtaining Documentation

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

## Cisco.com

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

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

You can access the Cisco website at this URL:

<http://www.cisco.com>

You can access international Cisco websites at this URL:

[http://www.cisco.com/public/countries\\_languages.shtml](http://www.cisco.com/public/countries_languages.shtml)

## Product Documentation DVD

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

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

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

Cisco Ordering tool:

<http://www.cisco.com/en/US/partner/ordering/>

Cisco Marketplace:

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

## Ordering Documentation

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

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

Cisco will continue to support documentation orders using the Ordering tool:

- Registered Cisco.com users (Cisco direct customers) can order documentation from the Ordering tool:  
<http://www.cisco.com/en/US/partner/ordering/>
- Instructions for ordering documentation using the Ordering tool are at this URL:  
[http://www.cisco.com/univercd/cc/td/doc/es\\_inpk/pdi.htm](http://www.cisco.com/univercd/cc/td/doc/es_inpk/pdi.htm)
- Nonregistered Cisco.com users can order documentation through a local account representative by calling Cisco Systems Corporate Headquarters (California, USA) at 408 526-7208 or, elsewhere in North America, by calling 1 800 553-NETS (6387).

## Documentation Feedback

You can rate and provide feedback about Cisco technical documents by completing the online feedback form that appears with the technical documents on Cisco.com.

You can send comments about Cisco documentation to [bug-doc@cisco.com](mailto:bug-doc@cisco.com).

You can submit comments by using the response card (if present) behind the front cover of your document or by writing to the following address:

Cisco Systems  
Attn: Customer Document Ordering  
170 West Tasman Drive  
San Jose, CA 95134-9883

We appreciate your comments.

## Cisco Product Security Overview

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

[http://www.cisco.com/en/US/products/products\\_security\\_vulnerability\\_policy.html](http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html)

From this site, you can perform these tasks:

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

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

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

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

[http://www.cisco.com/en/US/products/products\\_psirt\\_rss\\_feed.html](http://www.cisco.com/en/US/products/products_psirt_rss_feed.html)

## Reporting Security Problems in Cisco Products

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

- Emergencies — [security-alert@cisco.com](mailto:security-alert@cisco.com)

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

- Nonemergencies — [psirt@cisco.com](mailto:psirt@cisco.com)

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

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



Tip

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

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

[http://www.cisco.com/en/US/products/products\\_security\\_vulnerability\\_policy.htm](http://www.cisco.com/en/US/products/products_security_vulnerability_policy.htm)

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

---

## Obtaining Technical Assistance

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

### Cisco Technical Support and Documentation Website

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

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

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

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



#### Note

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

---

## Submitting a Service Request

Using the online TAC Service Request Tool is the fastest way to open S3 and S4 service requests. (S3 and S4 service requests are those in which your network is minimally impaired or for which you require product information.) After you describe your situation, the TAC Service Request Tool provides recommended solutions. If your issue is not resolved using the recommended resources, your service request is assigned to a Cisco engineer. The TAC Service Request Tool is located at this URL:

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

For S1 or S2 service requests or if you do not have Internet access, contact the Cisco TAC by telephone. (S1 or S2 service requests are those in which your production network is down or severely degraded.) Cisco engineers are assigned immediately to S1 and S2 service requests to help keep your business operations running smoothly.

To open a service request by telephone, use one of the following numbers:

Asia-Pacific: +61 2 8446 7411 (Australia: 1 800 805 227)

EMEA: +32 2 704 55 55

USA: 1 800 553-2447

For a complete list of Cisco TAC contacts, go to this URL:

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

## Definitions of Service Request Severity

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

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

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

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

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

## Obtaining Additional Publications and Information

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

- Cisco Marketplace provides a variety of Cisco books, reference guides, documentation, and logo merchandise. Visit Cisco Marketplace, the company store, at this URL:  
<http://www.cisco.com/go/marketplace/>
- *Cisco Press* publishes a wide range of general networking, training and certification titles. Both new and experienced users will benefit from these publications. For current Cisco Press titles and other information, go to Cisco Press at this URL:

<http://www.ciscopress.com>

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

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

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

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

or view the digital edition at this URL:

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

- *Internet Protocol Journal* is a quarterly journal published by Cisco Systems for engineering professionals involved in designing, developing, and operating public and private internets and intranets. You can access the Internet Protocol Journal at this URL:

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

- Networking products offered by Cisco Systems, as well as customer support services, can be obtained at this URL:

<http://www.cisco.com/en/US/products/index.html>

- Networking Professionals Connection is an interactive website for networking professionals to share questions, suggestions, and information about networking products and technologies with Cisco experts and other networking professionals. Join a discussion at this URL:

<http://www.cisco.com/discuss/networking>

- World-class networking training is available from Cisco. You can view current offerings at this URL:

<http://www.cisco.com/en/US/learning/index.html>

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

CCVP, the Cisco logo, and the Cisco Square Bridge logo are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn is a service mark of Cisco Systems, Inc.; and Access Registrar, Aironet, BPX, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, iQuick Study, LightStream, Linksys, MeetingPlace, MGX, Networking Academy, Network Registrar, PIX, ProConnect, ScriptShare, SMARTnet, StackWise, The Fastest Way to Increase Your Internet Quotient, and TransPath are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0709R)