



Catalyst 6500 Series Supervisor Engine Flash PC Card Installation Note

Product Numbers:

MEM-C6K-FLC16M(=)

MEM-C6K-FLC24M(=)

MEM-C6K-FLC64M(=)

MEM-C6K-ATA-1-64M(=)

This installation note contains the procedure to install a Flash PC card in the Catalyst 6500 series supervisor engines.



Note

The 64-MB ATA Flash PC card (MEM-C6K-ATA-1-64M) requires Supervisor Engine 2 with ROMMON software release 7.1(1) or later releases. For ROMMON software upgrade details, refer to http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/relnotes/78_13488.htm.

The ATA Flash PC card is supported on Catalyst 6500 series switches running Cisco IOS Release 12.1(8a)EX or later releases on both the supervisor engine and the Multilayer Switch Feature Card (MSFC).

The ATA Flash PC card is supported on Catalyst 6500 series switches running Catalyst software release 7.5(1) or later releases on the supervisor engine and Cisco IOS on the MSFC.



Note

The 64-MB linear Flash PC card (MEM-C6K-FLC64M) is supported only on Supervisor Engine 1 and requires ROMMON software release 5.3(1) or later releases.

The 64-MB linear Flash PC card is supported on Catalyst 6500 series switches running Cisco IOS Release 12.1(13)E4 or later releases on both the supervisor engine and the MSFC.

The 64-MB linear Flash PC card is supported on Catalyst 6500 series switches running Catalyst software release 7.5(1) or later releases on the supervisor engine and Cisco IOS software on the MSFC.



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

© 1999–2005 Cisco Systems, Inc. All rights reserved.

Contents

This installation note contains the following sections:

- [Supervisor Engine Flash PC Cards, page 2](#)
- [Preventing Electrostatic Discharge Damage, page 3](#)
- [Installing and Removing a Flash PC Card, page 3](#)
- [Using Flash PC Cards, page 6](#)
- [Additional Documentation, page 8](#)
- [Obtaining Documentation, page 8](#)
- [Documentation Feedback, page 9](#)
- [Cisco Product Security Overview, page 9](#)
- [Obtaining Technical Assistance, page 10](#)
- [Obtaining Additional Publications and Information, page 12](#)

Supervisor Engine Flash PC Cards

The supervisor engine Flash PC cards conform with the PCMCIA format. These models are available:

- 16-MB MEM-C6K-FLC16M
- 24-MB MEM-C6K-FLC24M
- 64-MB MEM-C6K-FLC64M
- MEM-C6K-ATA-1-64M



Note

The 16-MB MEM-C6K-FLC16M and 24-MB MEM-C6K-FLC24M linear Flash PC cards are formatted for the Catalyst 6500 series supervisor engines and are ready to use.

The MEM-C6K-ATA-1-64M and 64-MB MEM-C6K-FLC64M Flash PC cards *are not* formatted. You must format these cards (See [Table 1 on page 7 Commands for Using and Managing Flash Devices](#) [Table 1](#) for a description of the **format** command.) When you enter the **dir disk0:** or **dir slot0:** commands, an unformatted Flash PC card returns a “bad device block info” or “invalid magic number” error message.

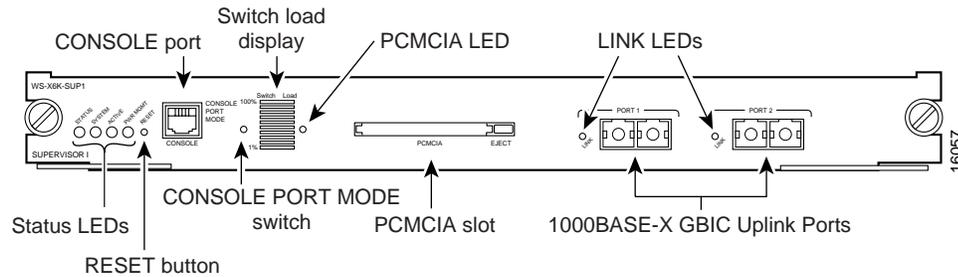


Note

Supervisor Engine 1 and Supervisor Engine 2 do not support the same Flash PC card format. To use a Flash PC card with Supervisor Engine 2, you must format the card with Supervisor Engine 2. To use a Flash PC card with Supervisor Engine 1, you must format the card with Supervisor Engine 1.

You can use Flash PC cards to store and boot software images, or they can be used as servers to store software images for other systems. You can configure each supervisor engine with one Flash PC card in slot 0. [Figure 1](#) shows the front panel of a supervisor engine with the single PCMCIA slot, slot 0.

Figure 1 Supervisor Engine Flash PC Card Slot



For information about using the PCMCIA Flash PC cards, see the [“Using Flash PC Cards”](#) section on page 6.

Preventing Electrostatic Discharge Damage

Follow these guidelines to prevent electrostatic discharge (ESD) damage:

- Always use an ESD wrist or ankle strap, and ensure that it makes good skin contact.
- Connect the equipment end of the strap to the ESD connector on the switch.
- Place a removed Flash PC card on an antistatic surface or in a static shielding bag. If the card will be returned to the factory, immediately place it in a static shielding bag.
- Avoid contact between the card and clothing. The wrist strap only protects the card from ESD voltages on the body; ESD voltages on clothing can still cause damage.



Caution

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

Installing and Removing a Flash PC Card

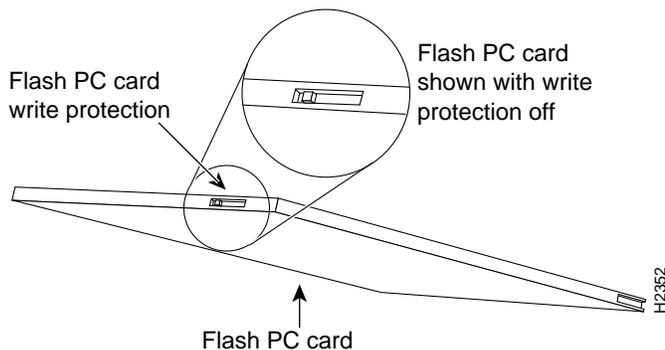
Before you install a Flash PC card, verify that the card’s write-protect switch is off. When the card is oriented with the printing side up and the edge connector end away from you, the write-protect switch is located on the front edge of the card, as shown in [Figure 2](#).



Note

Not all Flash PC cards have the write-protect switch.

Figure 2 Locating the Flash PC Card Write Protection Switch



To install and remove a Flash PC card (see [Figure 3](#)), perform these steps:



Note

You can insert and remove the Flash PC card with the power on.

- Step 1** Connect an ESD-preventive strap to the ESD connector on the switch.
- Step 2** Face the front panel of the switch, and hold the Flash PC card with the connector end toward the slot, as shown in [Figure 3a](#).
- Step 3** Insert the card into the slot until it completely seats in the connector at the back of the slot and the eject button pops out toward you, as shown in [Figure 3b](#).

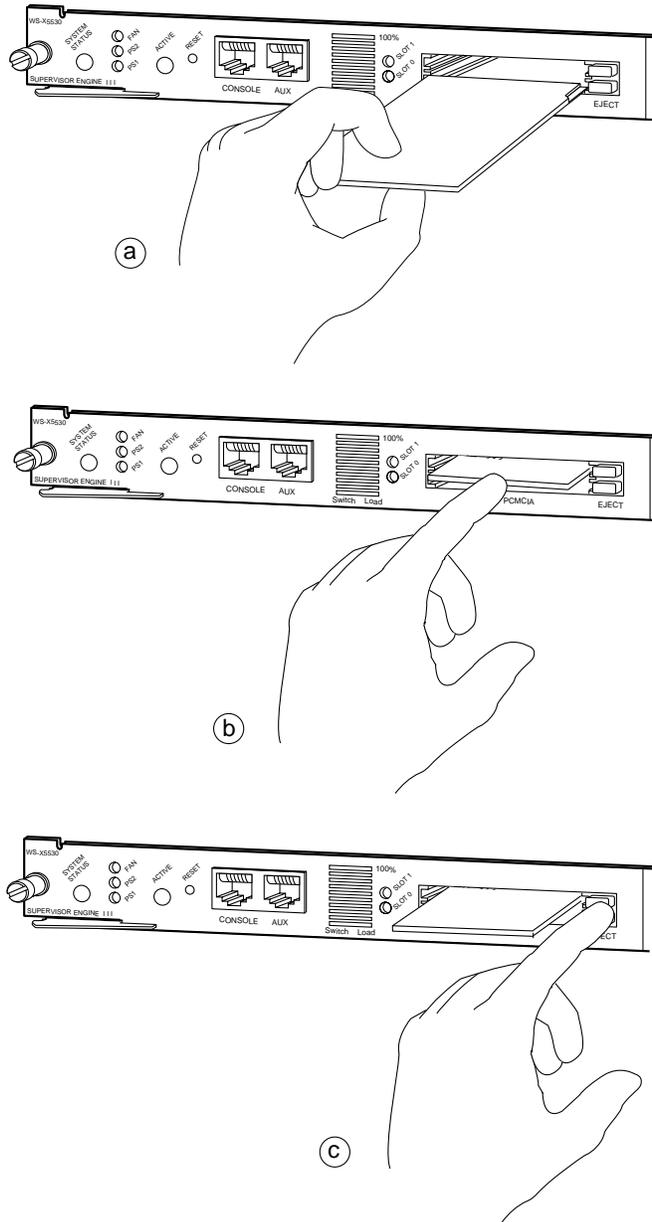


Note

The card does not insert all the way inside the slot; a portion of the card remains outside the slot. *Do not attempt to force the card past this point.*

- Step 4** To eject a Flash PC card, press the ejector button until the card is free of the connector at the back of the slot, as shown in [Figure 3c](#).
- Step 5** Remove the card from the slot and place it in an antistatic bag.

Figure 3 Installing and Removing a Flash PC Card



14233

Using Flash PC Cards


Note

An MS-DOS formatted ATA Flash PC card or linear Flash PC card can be accessed successfully (including the **dir** command) with the Catalyst and Cisco IOS operating systems but will not boot from ROMMON.


Note

The 16-MB MEM-C6K-FLC16M and 24-MB MEM-C6K-FLC24M linear Flash PC cards are formatted for the Catalyst 6500 series supervisor engines and are ready to use.

The MEM-C6K-ATA-1-64M and 64-MB MEM-C6K-FLC64M Flash PC cards *are not* formatted. You must format these cards (see [Table 1 on page 7](#) for a description of the **format** command.) When you enter the **dir disk0:** or **dir slot0:** commands, an unformatted Flash PC card returns a “bad device block info” or “invalid magic number” error message.


Note

Supervisor Engine 1 and Supervisor Engine 2 do not support the same Flash PC card format. To use a Flash PC card with Supervisor Engine 2, you must format the card with Supervisor Engine 2. To use a Flash PC card with Supervisor Engine 1, you must format the card with Supervisor Engine 1.

[Table 1](#) [Table 1](#) [Table 1](#) [Table 1](#) shows many of the commands that are available for using and managing Flash devices, including the Flash PC cards. To perform specific tasks, use these commands either alone or combined with other commands. For example, to copy a file from a TFTP server to a Flash PC card, set the BOOT environment variable so that the system will boot from this new image and then verify the boot sequence as shown in the following steps:


Note

The following commands listed in [Table 1](#) are not applicable to the ATA Flash (disk0:) PC card: **undelete**, **squeeze**, **show flash devices**, **show flash**, and **verify**.


Note

The ATA Flash PC card is accessed through disk0: and the 16-MB, 24-MB, and 64-MB Flash PC cards are accessed through slot0:. The following procedure uses slot0:.

Step 1 Copy a file from a TFTP server to the Flash PC card in slot0:

```
Console (enable) copy tftp slot0:
```

Step 2 Set the BOOT environment variable so that the system boots from slot0:

```
Console (enable) set boot system flash slot0:cat6000-sup-5-1-1-CSX.bin prepend
```

Step 3 Display the contents of the BOOT environment variable:

```
Console (enable) show boot
```

For complete descriptions of these commands and how to use them, refer to the *Catalyst 6500 Series Software Configuration Guide* and the *Catalyst 6500 Series Command Reference* publication.

Table 1 *Commands for Using and Managing Flash Devices*

Task	Command
Copy a Flash file to a TFTP server, another Flash device, or to the running configuration.	copy <i>m/device:filename</i> { tftp flash <i>m/device:filename</i> config }
Copy a file from a TFTP server to a Flash device or to the running configuration.	copy tftp { flash <i>m/device:filename</i> config }
Copy a file from Flash memory to a TFTP server or to a Flash device, or to the running configuration.	copy flash { tftp <i>m/device:filename</i> config }
Copy the running configuration to another Flash device or to a TFTP server.	copy config { flash <i>m/device:filename</i> tftp }
Set the BOOT environment variable.	set boot system flash <i>device:[filename]</i> [prepend] [<i>mod_num</i>]
Format a Flash PC device.	format [<i>spare spare-number</i>] [<i>m/</i>] <i>device1</i> : [[<i>device2</i> :] [<i>monlib-filename</i>]]
Specify the boot field in the configuration register, which determines the boot method the switch will use at the next startup.	set boot config-register boot { rommon bootflash system } [<i>mod_num</i>]
Display the contents of the BOOT environment variable.	show boot [<i>mod_num</i>]
Clear a specific image from the BOOT environment variable.	clear boot system flash <i>device:[filename]</i> [<i>mod_num</i>]
Clear the entire BOOT environment variable.	clear boot system all [<i>mod_num</i>]
Display a list of files on a Flash device.	dir [[<i>m/</i>] <i>device:</i>] <i>filename</i>] [all deleted long]
Set the default Flash device for the system.	cd [[<i>m/</i>] [bootflash: slot0:]]
Verify the default Flash device for the system.	pwd [<i>mod_num</i>]
Delete a file on a Flash device.	delete [[<i>m/</i>] <i>device:</i>] <i>filename</i>
Undelete a file on a Flash device.	undelete <i>index</i> [[<i>m/</i>] <i>device:</i>]
Permanently remove all deleted files on a Flash device.	squeeze [<i>m/</i>] <i>device:</i>
Identify the supported Flash devices on the system.	show flash devices
Display information about the Flash PC.	show flash [[<i>m/</i>] <i>device:</i>] [all chips filesystem]
Verify the checksum of a file on a Flash device.	verify [[<i>m/</i>] <i>device:</i>] <i>filename</i>

Additional Documentation

Refer to the following documents for additional information on supervisor engine Flash devices:

- *Release Notes for Catalyst 6500 Series and Cisco 7600 Series Internet Router Supervisor Engine 2 ROMMON*
- *Catalyst 6500 Series Software Configuration Guide*
- *Catalyst 6500 Series Command Reference*

Obtaining Documentation

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

Cisco.com

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

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

You can access the Cisco website at this URL:

<http://www.cisco.com>

You can access international Cisco websites at this URL:

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

Product Documentation DVD

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

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

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

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

Ordering Documentation

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

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

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

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.

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

From this site, you can perform these tasks:

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

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

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

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

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

Reporting Security Problems in Cisco Products

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

- Emergencies—security-alert@cisco.com

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

- Nonemergencies—psirt@cisco.com

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

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



Tip

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

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

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

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

Obtaining Technical Assistance

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

Cisco Technical Support & Documentation Website

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

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

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

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

**Note**

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

Submitting a Service Request

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 *Catalyst 6500 Series Software Configuration Guide* and the *Catalyst 6500 Series Command Reference* publications.

CCSP, CCVP, the Cisco Square Bridge logo, Follow Me Browsing, and StackWise are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn, and iQuick Study are service marks of Cisco Systems, Inc.; and Access Registrar, Aironet, ASIST, BPX, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Empowering the Internet Generation, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, FormShare, GigaDrive, GigaStack, HomeLink, Internet Quotient, IOS, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, LightStream, Linksys, MeetingPlace, MGX, the Networkers logo, Networking Academy, Network Registrar, *Packet*, PIX, Post-Routing, Pre-Routing, ProConnect, RateMUX, ScriptShare, SlideCast, SMARTnet, StrataView Plus, TeleRouter, 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. (0502R)

Copyright © 1999–2005, Cisco Systems, Inc.
All rights reserved.