



Release Notes for Cisco Unified MeetingPlace SMTP E-Mail Gateway Release 5.3

Revised: May 10, 2006, OL-6770-02

These release notes describe the new features and caveats for all versions of Cisco Unified MeetingPlace SMTP E-Mail Gateway Release 5.3.

You can access the latest software upgrades and release notes for all versions of Cisco Unified MeetingPlace SMTP E-Mail Gateway on Cisco Connection Online (CCO) at the following URL:

<http://www.cisco.com/univercd/cc/td/doc/product/conf/mtgplace/smtp/530/index.htm>

Contents

These release notes discuss the following topics:

- [Introduction, page 2](#)
- [System Requirements, page 2](#)
- [Cisco Unified MeetingPlace Product Compatibility, page 3](#)
- [Related Documentation, page 3](#)
- [New and Changed Information, page 4](#)
- [Installation Notes, page 4](#)
- [Caveats, page 4](#)
- [Obtaining Documentation, page 10](#)
- [Documentation Feedback, page 11](#)
- [Cisco Product Security Overview, page 11](#)
- [Obtaining Technical Assistance, page 12](#)
- [Obtaining Additional Publications and Information, page 13](#)



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

© 2004-2006 Cisco Systems, Inc. All rights reserved.

Introduction

This document describes Cisco Unified MeetingPlace SMTP E-Mail Gateway Release 5.3 and includes system requirements, new features, and outstanding caveats.

System Requirements

New installations of the Cisco Unified MeetingPlace SMTP E-Mail Gateway Release 5.3 require a Cisco Media Convergence Server (MCS) dedicated to Cisco Unified MeetingPlace applications. Hardware configuration is based on the number of voice and web-conferencing user licenses (ports) on your system.

Upgrading to Release 5.3 requires a Cisco MCS or exact HP or IBM equivalent. If you are not using an exact HP or IBM equivalent, you must install Release 5.3 as a new installation on a supported Cisco MCS.

[Table 1](#) provides information about system requirements for the Cisco Unified MeetingPlace SMTP E-Mail Gateway Release 5.3.

Table 1 *Cisco Unified MeetingPlace SMTP E-Mail Gateway Requirements*

System	Requirement
Cisco MCS Unified CallManager Appliance (Cisco MCS)	<p>Hardware</p> <ul style="list-style-type: none"> A Cisco MCS, or the exact equivalent from HP or IBM, that is dedicated to Cisco Unified MeetingPlace applications. <p>Version utility</p> <ul style="list-style-type: none"> Sun Java Runtime Environment (JRE)1.4.2_05 <p>Operating System</p> <ul style="list-style-type: none"> Cisco MCS OS Image 2000.2.7 Cisco MCS OS Service Release 2000.2.7 Cisco MCS OS Upgrade 2000.2.7
Network requirements	<ul style="list-style-type: none"> Microsoft Windows 2000 server or later version Hardware <ul style="list-style-type: none"> 64 MB RAM or better 15 MB free disk space plus 100 MB of additional space for temporary files like attachments and notifications 233 MHz Pentium II processor TCP/IP connection to the Cisco Unified MeetingPlace Audio Server using a static IP address

Table 1 Cisco Unified MeetingPlace SMTP E-Mail Gateway Requirements (continued)

System	Requirement
Cisco Unified MeetingPlace Audio Server	<p>Hardware</p> <ul style="list-style-type: none"> • Cisco Unified MeetingPlace 8112 or Cisco Unified MeetingPlace 8106 <p>Software</p> <ul style="list-style-type: none"> • Cisco Unified MeetingPlace Audio Server Release 5.3 <p>Other</p> <ul style="list-style-type: none"> • Cisco MeetingPlace Notification Option (required for distributing meeting notifications) • Cisco MeetingPlace MeetingNotes Data Option (required for distributing meeting attachments)
Option key	The Cisco Unified MeetingPlace system option must be enabled for your corporate e-mail system. For Microsoft Mail, Microsoft Exchange, and other MAPI-compliant e-mail systems, the option key name is E-Mail Gateway (SMTP).
E-mail system	<p>SMTP-based, supported mail system (such as Microsoft Exchange or Lotus Domino).</p> <p>If authentication is required on your corporate SMTP e-mail server, create an authorized account on your corporate e-mail system for the Cisco Unified MeetingPlace SMTP E-Mail Gateway to use.</p> <p>Verify that you have a personal e-mail account. You will need an e-mail account to test the Cisco Unified MeetingPlace SMTP E-Mail Gateway.</p>

Cisco Unified MeetingPlace Product Compatibility

For information about the interoperability among the Cisco Unified MeetingPlace products, see the “Cisco Unified MeetingPlace Product Compatibility Matrix” section of the *Installation Planning Guide* for Cisco Unified MeetingPlace Release 5.3 at the following URL:

http://www.cisco.com/en/US/products/sw/ps5664/ps5669/prod_installation_guides_list.html

Cisco Security Agent

Cisco Unified MeetingPlace SMTP E-Mail Gateway Release 5.3 is not compatible with Cisco Security Agent (CSA). We recommend that you do not install Cisco Security Agent on a gateway server where Cisco Unified MeetingPlace SMTP E-Mail Gateway Release 5.3 is or will be installed.

If Cisco Security Agent is installed on an end-user system, users will see a security alert when they attempt to use the application-sharing feature. Users can choose to proceed with the feature and use application-sharing without difficulty.

Related Documentation

For additional information about Cisco Unified MeetingPlace products or about obtaining documentation or technical support, see the *Guide to Cisco Conferencing Documentation and Support* at the following URL:

http://www.cisco.com/en/US/products/sw/ps5664/ps5669/products_documentation_roadmaps_list.html

New and Changed Information

Topics in this section include:

- [New Features in Release 5.3\(0.68\)](#), page 4
- [New Features in Release 5.3\(0.60\)](#), page 4
- [New Features in Release 5.3\(0.53\)](#), page 4

New Features in Release 5.3(0.68)

This release includes bug fixes. There are no new features in this release.

New Features in Release 5.3(0.60)

This release includes bug fixes. There are no new features in this release.

New Features in Release 5.3(0.53)

This release provides localized strings to support French, German, Portuguese (Brazil), and Spanish (Latin America).

Installation Notes



Note

We recommend that you install the Cisco Unified MeetingPlace SMTP E-Mail Gateway after installing Cisco Unified MeetingPlace Web Conferencing. See the Cisco Unified MeetingPlace Web Conferencing documentation set for more information about installing Cisco Unified MeetingPlace Web Conferencing.

Upgrading a legacy Cisco MeetingPlace SMTP E-Mail Gateway system (such as Release 4.3) to Cisco Unified MeetingPlace SMTP E-Mail Gateway Release 5.3 requires a legacy third-party Windows server with system specifications comparable to Cisco MCS specifications required for the same deployment. For information on Cisco MCS specifications, see the following URL:

<http://www.cisco.com/en/US/partner/products/hw/voiceapp/ps378/index.html>

Caveats

You can find the latest resolved caveat information for Cisco Unified MeetingPlace SMTP E-Mail Gateway Release 5.3 by using Bug Toolkit, which is an online tool that is available for customers to query defects according to their own needs.

**Tip**

You need an account with Cisco.com (Cisco Connection Online) to use the Bug Toolkit to find open and resolved caveats of any severity for any release.

To access the Bug Toolkit, log onto http://www.cisco.com/cgi-bin/Support/Bugtool/launch_bugtool.pl.

This section includes the following topics:

- [Using Bug Toolkit, page 5](#)
- [Saving Bug Toolkit Queries, page 6](#)
- [Open Caveats, page 7](#)
- [Resolved Caveats—Release 5.3\(0.68\), page 7](#)
- [Resolved Caveats—Release 5.3\(0.60\), page 8](#)

Using Bug Toolkit

To access Bug Toolkit, you need the following items:

- Internet connection
- Web browser
- Cisco.com user ID and password

To use Bug Toolkit, follow this procedure.

Procedure

-
- Step 1** To access the Bug Toolkit, go to http://www.cisco.com/cgi-bin/Support/Bugtool/launch_bugtool.pl.
- Step 2** Log on with your Cisco.com user ID and password.
- Step 3** Click the **Launch Bug Toolkit** hyperlink.
- Step 4** If you are looking for information about a specific caveat, enter the ID number in the “Enter known bug ID:” field.
- To view all caveats for Cisco Unified MeetingPlace, go to the “Search for bugs in other Cisco software and hardware products” section, and enter **Cisco MeetingPlace** in the Product Name field. Alternatively, you can scroll through the product name list and click **Cisco MeetingPlace**.
- Step 5** Click **Next**. The Cisco MeetingPlace search window displays.
- Step 6** Choose the filters to query for caveats. You can choose any or all of the available options:
- a. Choose the Cisco Unified MeetingPlace version:
 - Choose the major version for the major releases (such as 5.2 or 5.3).
A major release contains significant new features, enhancements, architectural changes, and/or defect fixes.
 - Choose the revision for more specific information.
A revision (maintenance) release primarily contains defect fixes to address specific problems, but it may also include new features and/or enhancements.
 - b. Choose the Features or Components to query; make your selection from the “Available” list and click Add to place your selection in the “Limit search to” list.

- To query for all Cisco Unified MeetingPlace caveats for a specified release, choose “All Features” in the left window pane.



Note The default value specifies “All Features” and includes all of the items in the left window pane.

- To query only for Cisco Unified MeetingPlace-related caveats, choose “ciscoxm” and then click **Add**.
- c. Enter keywords to search for a caveat title and description, if desired.



Note To make queries less specific, use the All wildcard for the major version/revision, features/components, and keyword options.

- d. Choose the Set Advanced Options, including the following items:
- Bug Severity level—The default specifies 1-3.
 - Bug Status Group—Check the **Fixed** check box for resolved caveats.
 - Release Note Enclosure—The default specifies Valid Release Note Enclosure.
- e. Click **Next**.

Bug Toolkit returns the list of caveats on the basis of your query.

- You can modify your results by submitting another query and using different criteria.
- You can save your query for future use. See the [“Saving Bug Toolkit Queries” section on page 6](#).



Note For detailed online help with Bug Toolkit, click **Help** on any Bug Toolkit window.

Saving Bug Toolkit Queries

Bug Toolkit allows you to create and then save your queries to monitor a specific defect or network situation. You can edit a saved search at any time to change the alert conditions, the defects being watched, or the network profile.

Follow this procedure to save your Bug Toolkit queries.

Procedure

- Step 1** Perform your search for caveats, as described in the [“Using Bug Toolkit” section on page 5](#).
- Step 2** In the search result window, click the **This Search Criteria** button that displays at the bottom of the window.
- A new window displays.
- Step 3** In the Name of saved search field, enter a name for the saved search.
- Step 4** Under My Bug Groups, use one of the following options to save your defects in a bug group:
- Click the **Existing group** radio button and choose an existing group name from the drop-down list box.

- Click the **Create new group named:** radio button and enter a group name to create a new group for this saved search.



Note This bug group will contain the bugs that are identified by using the search criteria that you have saved. Each time that a new bug meets the search criteria, the system adds it to the group that you chose.

Bug Toolkit saves your bugs and searches, and makes them available through the My Stuff window. (The My Stuff window allows you to view, create, and/or modify existing bug groups or saved searches. Choose the My Stuff link to see a list of all your bug groups.)

- Step 5** Under Email Update Options, you can choose to set optional e-mail notification preferences if you want to receive automatic updates of a bug status change. Bug Toolkit provides the following options:
- **Do NOT send me any email updates**—If you choose this default setting, Bug Toolkit does not send e-mail notifications.
 - **Send my updates to:**—Click the radio button to choose this option to send e-mail notifications to the user ID that you enter in this field. Additional notification options include:
 - **Updates as they occur**—Bug Toolkit provides updates that are based on status change.
 - **Weekly summaries**—Bug Toolkit provides weekly summary updates.
 - **Apply these email update options to all of my saved searches**—Check this check box to use these e-mail update options for all of your saved searches.
- Step 6** To save your changes, click **Save**.
- Step 7** A window displays the bug group(s) that you have saved. From this window, you can click a bug group name to see the bugs and the saved searches; you can also edit the search criteria.

Open Caveats

This section describes possible unexpected behaviors by Cisco Unified MeetingPlace SMTP E-Mail Gateway Release 5.3. Only severity 1, severity 2, and select severity 3 open caveats are provided in this document. Unless otherwise noted, these caveats apply to all Cisco Unified MeetingPlace SMTP E-Mail Gateway 5.3 releases up to and including release 5.3(0.68).

There are no open caveats for Cisco Unified MeetingPlace SMTP E-Mail Gateway Release 5.3.

Resolved Caveats—Release 5.3(0.68)

[Table 2](#) lists caveats that are resolved in Cisco Unified MeetingPlace SMTP E-Mail Gateway Release 5.3(0.68) but that may be open in previous releases. Only severity 1, severity 2, and select severity 3 resolved caveats are provided in this document, and they are listed in alphanumeric order by bug identifier. For more information about an individual defect, click or go to the URL in [Table 2](#) to access the online record for that defect.

Because defect status continually changes, be aware that [Table 2](#) reflects a snapshot of the defects that were resolved at the time this report was compiled. For an updated view of resolved defects, access Bug Toolkit at http://www.cisco.com/cgi-bin/Support/Bugtool/launch_bugtool.pl. Bug Toolkit requires that you have an account with Cisco.com (Cisco Connection Online).

Table 2 *Resolved Caveats in Cisco Unified MeetingPlace SMTP E-Mail Gateway Release 5.3(0.68)*

Identifier	Headline
CSCsb75300	Browser test from Notification is running on English for all languages http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCsb75300
CSCsb78532	Participant list is not included in the notification http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCsb78532
CSCsb79289	E-mail / To change Date/Time back to America time standard http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCsb79289
CSCsc09080	No Show/Renew Notification titles displayed on English (Japanese) http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCsc09080
CSCsc18943	gwsim status does not display correct version of SMTP after installation http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCsc18943

Resolved Caveats—Release 5.3(0.60)

Table 3 *Resolved Caveats in Cisco Unified MeetingPlace SMTP E-Mail Gateway Release 5.3(0.60)*

Identifier	Headline
CSCsa36224	MPWeb DC slave disassociated from master servlet and could not reconnect
CSCsa61827	MPWeb - MCS OS 2000.2.6.SR7 gives Overlapped I/O in progress message
CSCsa87103	Inetinfo crash in comsvcs.dll triggered by Web Polling
CSCsa87108	Inetinfo crash in wam.dll
CSCsa97262	Dataconference server master / slave disconnection
CSCsb03155	MP Agent crash in function GenerateHTMLFromList
CSCsb03746	gwsvc crash in PartyMapper::destroyAllParties
CSCsb37025	MPAgent crash in cgpiapi when terminating conference
CSCsa32873	Powerpoint filenames with accent mark do not load in Meeting Room
CSCsa52178	SQL db corruption cause FIND meeting problems
CSCsa61394	MeetingPlace Audio Service leaking memory, handles and threads
CSCsa63990	User prompted for new password on the web is denied entry
CSCsa66052	User whose profile pwd expired cannot join mtg or access other features
CSCsa93586	4 second delay between voice and data in web recording
CSCsb00918	Audio in web recording playback contains slight pauses/dead-air
CSCsb25476	Cannot access attachments from attachments tab in Meeting Console
CSCsb65208	NetMeeting users showed up as participants in mtgs they've never joined
CSCsb81561	Load balancing broken, cannot assign meeting to the right server
CSClt20786	Stale guest session leads to launching slide show with wrong conference

Table 3 *Resolved Caveats in Cisco Unified MeetingPlace SMTP E-Mail Gateway Release 5.3(0.60) (continued)*

Identifier	Headline
CSCIt21132	Browser test not detecting unsupported version of JVM
CSCIt22226	Session has expired appears after clicking cancel in MSM sched pg
CSCIt22566	Attachment Location in db blank - attachment folders created under WINNT
CSCIt22901	User whose ID contains & character unable to sched from MPOL
CSCed95973	Poll window missing buttons to create polls when username contains blank
CSCee52173	NT App log ERROR: Cannot insert NULL to column customerID
CSCsa31625	Uninstall MPWeb that used shared SQL db does not remove its ref in db
CSCsa39994	Unexpected error when deleting meeting series from Outlook
CSCsa40510	User whose NT account contains Japanese char unable to share in DC
CSCsa54050	Web agent does not recognize mpserver option keys
CSCsa71963	Webshare on Mac OS10 Safari "Click here for help" link broken
CSCsa85092	Windows performance monitor counters not working
CSCsa97632	MPWeb upgrade from 4.3 to 5.3 did not update NumSession value in registry
CSCsb07092	Browser Test does not detect IE 5.5 SP2 installed
CSCsb17304	Participant list shows username instead of FirstName LastName
CSCsb32027	Attachments added always by same user, same date
CSCsb40560	MeetingPlace Web Administration GUI reverts to default values
CSCsb43684	Change install option from BOTH Full Access to BOTH SMA-1S
CSCsb52751	Reference Center material outdated - only 4.3 but need 5.3
CSCsb64283	Duplicate strings in html code results in confusion in updating values
CSCsb82485	Meeting Console window white screen if using SUN JRE 1.4.2_03 & below
CSCsa56091	Admin unable to hide MeetingNotes from user interface
CSCsb60735	Fix misspelled words on DMZ Home Page
CSCsa71403	help@yourcompany.com in reference center is displayed and does not change
CSCsa89154	Users allowed to attempt outdial from Meeting Room when outdial has been disabled
CSCIt21666	Admin page displayed in mixed English and French
CSCIt22280	Language choice must be kept after guest sign-in when attending meeting
CSCsa46919	SDK does not return common id to match User Participant and Invitee
CSCsa81932	Browser test should detect pop up blocker
CSCsa98794	CTA not working if Split DNS and only DMZ using SSL
CSCsb00832	Enhance eventlog to display clearer, more accurate SQL related errors

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/univercd/home/home.htm>

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

Documentation DVD

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

Registered Cisco.com users (Cisco direct customers) can order a Cisco 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

You can find instructions for ordering documentation at this URL:

http://www.cisco.com/univercd/cc/td/doc/es_inpk/pdi.htm

You can order Cisco documentation in these ways:

- Registered Cisco.com users (Cisco direct customers) can order Cisco product documentation from the Ordering tool:
<http://www.cisco.com/en/US/partner/ordering/>
- 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 send comments about technical 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
- Nonemergencies—psirt@cisco.com



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 that has the most recent creation date in this public key server list:

<http://pgp.mit.edu:11371/pks/lookup?search=psirt%40cisco.com&op=index&exact=on>

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

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

Obtaining Technical Assistance

For all customers, partners, resellers, and distributors who hold valid Cisco service contracts, Cisco Technical Support provides 24-hour-a-day, award-winning technical assistance. The Cisco Technical Support Website on Cisco.com features extensive online support resources. In addition, Cisco Technical Assistance Center (TAC) engineers provide telephone support. If you do not hold a valid Cisco service contract, contact your reseller.

Cisco Technical Support Website

The Cisco Technical Support 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, 365 days a year, at this URL:

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

Access to all tools on the Cisco Technical Support 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 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 TAC 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 TAC 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, 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>

- *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>

- 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 documents listed in the “[Related Documentation](#)” section.

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, *Packet*, 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. (0705R)

©2004-2006 Cisco Systems, Inc. All rights reserved.