



Release Note for Cisco Wide Area Application Services

May 6, 2008



Note

The most current Cisco documentation for released products is also available on [cisco.com](http://www.cisco.com). The online documents may contain updates and modifications made after the hardcopy documents were released.

Contents

This release note applies to Cisco Wide Area Application Services (WAAS) software version 4.0.9. For information on WAAS features and commands, refer to the WAAS documentation located at http://www.cisco.com/en/US/products/ps6870/tsd_products_support_series_home.html.

This release note contains the following sections:

- [WAAS Product Overview](#)
- [Changed Default Behavior for EPM Classification](#)
- [Upgrading From WAFS to WAAS](#)
- [Upgrading from a Prerelease Version to Version 4.0.9](#)
- [Upgrading from Version 4.0.x to 4.0.9](#)
- [Operating Considerations](#)
- [Documentation Enhancements and Corrections](#)
- [Software Version 4.0.9 Open and Resolved Caveats](#)
- [Obtaining Documentation and Submitting a Service Request](#)



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

© 2007-2008 Cisco Systems, Inc. All rights reserved.

WAAS Product Overview

The WAAS system consists of a set of devices called wide area application engines (WAEs) that work together to optimize TCP traffic over your network. When client and server applications attempt to communicate with each other, the network intercepts and redirects this traffic to the WAEs so they can act on behalf of the client application and the destination server. The WAEs examine the traffic and use built-in application policies to determine whether to optimize the traffic or allow it to pass through your network unoptimized.

You can use the WAAS Central Manager GUI to centrally configure and monitor the WAEs and application policies in your network. You can also use the WAAS Central Manager GUI to create new application policies so that the WAAS system can optimize custom applications and less common applications.

Cisco WAAS helps enterprises meet the following objectives:

- Provide branch office employees with LAN-like access to information and applications across a geographically distributed network.
- Migrate application and file servers from branch offices into centrally managed data centers.
- Minimize unnecessary WAN bandwidth consumption through the use of advanced compression algorithms.
- Provide print services to branch office users. WAAS allows you to configure a WAE as a print server so you do not need to deploy a dedicated system to fulfill print requests.
- Improve application performance over the WAN by addressing the following common issues:
 - Low data rates (constrained bandwidth)
 - Slow delivery of frames (high network latency)
 - Higher rates of packet loss (low reliability)

Changed Default Behavior for EPM Classification

The EPM Classification feature (EPM adaptor) has been disabled by default in WAAS 4.0.9. This feature is disabled on new software installations. The new default becomes effective after you upgrade to WAAS 4.0.9 from any version or when you use the **restore factory defaults** command.

The following comment appears in the WAAS 4.0.9 running config when the EPM adaptor is in the default state:

```
! adapter epm is disabled by default.
```

To enable the EPM Classification feature in WAAS 4.0.9, use the **adapter epm enable** global configuration command.

Upgrading From WAFS to WAAS

Although WAFS to WAAS migration is supported, rollback from WAAS to WAFS is not supported. For information regarding a WAFS-to-WAAS migration, contact your Cisco Sales Engineer.

If you are upgrading from WAFS 3.0.7 or later to WAAS, you must upgrade to a release version of WAAS 4.0.x only; you cannot upgrade to a prerelease version of 4.0.x.

If you are upgrading from the WAFS 3.0.7-special5 build or from a later WAFS release to WAAS, you must upgrade to a minimum of WAAS 4.0.5 or later; however, to ensure that you obtain all of the latest fixes and features, we recommend that you upgrade to the most current release of WAAS.

Upgrading from a Prerelease Version to Version 4.0.9

To upgrade from WAAS prerelease software to version 4.0.9, you must perform one of the following tasks to ensure a successful upgrade:

- Restore the factory default settings by using the **restore factory-default** command.
- Perform a fresh install from the rescue CD.

Upgrading from Version 4.0.x to 4.0.9

When you upgrade from version 4.0.x to version 4.0.9, observe the following guidelines and requirements:

- To take advantage of bug fixes and new features, we recommend that you upgrade your entire deployment to the latest software release.
- Before you upgrade your WAE, you must run a script (the WAAS disk check tool) that checks the file system for errors that can result from a RAID synchronization failure. See the [“Running the WAAS Disk Check Tool” section on page 3](#).
- Upgrade the WAE devices first, and then upgrade the WAE Central Manager devices last.
- If you operate a network with devices that have different software versions, the WAAS Central Manager should be the lowest version.
- When you upgrade edge and core devices, the CIFS-non-wafs classifier remains. If your Central Manager is operating at a lower version, you must manually delete the CIFS-non-wafs classifier and its policy map.

To delete the CIFS-non-wafs classifier using the Central Manager GUI, follow these steps:

-
- Step 1** Choose **Devices > Devices (or Device Groups) > Acceleration > Policies > Definitions**.
 - Step 2** Click the **Edit** icon next to the CIFS-non-wafs policy.
 - Step 3** Click **Edit Classifier**. The Modifying Application Classifier window appears.
 - Step 4** To delete the classifier and its policy, click the **Trash** icon.
-

- When you upgrade the Central Manager to version 4.0.9, the CIFS-non-wafs classifier is removed from edge and core devices automatically.

Running the WAAS Disk Check Tool

Before you upgrade your WAE from version 4.0.3 or earlier, you must run a script (the WAAS disk check tool) that checks the file system for errors that can result from a RAID synchronization failure. (For more information about RAID synchronization, see the [“About RAID Synchronization and File System](#)

Errors” section on page 4.) This script is not necessary when upgrading from WAAS version 4.0.5 or later, unless the system was running version 4.0.3 or earlier at some time in the past and the script was never run.

You can obtain the WAAS disk check tool from the following URL:

<http://www.cisco.com/cgi-bin/tablebuild.pl/waas40>



Note

When you run the WAAS disk check tool, you will be logged out of the device. The device automatically reboots after it has completed checking the file system. Because this operation results in a reboot, we recommend that you perform this operation after normal business hours.

Copy the script to your WAE device by using the **copy ftp disk** command.

```
WAE# copy ftp disk <ftp-server> <remote_file_dir> disk_check.sh
```

Run the script from the CLI, as shown in the following example:

```
WAE# script execute disk_check.sh
This script will check if there is any file system issue on the attached disks
Activating the script will result in:
Stopping all services. This will log you out.
Perform file system check for few minutes.
and record the result in the following files:
/local1/disk_status.txt - result summary
/local1/disk_check_log.txt - detailed log
System reboot
If the system doesn't reboot in 10 minutes, please re-login and check the result files.
Continue?[yes/no] yes
Please disk_status.txt after reboot for result summary
umount: /state: device is busy
umount: /local1/PAM_unix[26162]: ### pam_unix: pam_sm_close_session (su) session closed
for user root
waitpid returns error: No child processes
No child alive.
```

After the device reboots and you log in, locate and open the following two files to view the file system status:

- **disk_status.txt**— Lists each file system and shows if it is “OK,” or if it contains an error that requires attention.
- **disk_check_log.txt**—Contains a detailed log for each file system checked.

If no repair is needed, then each file system will be listed as “OK,” as shown in the following example:

```
WAE# type disk_status.txt
Thu Feb 1 00:40:01 UTC 2007
device /dev/md1 (/swstore) is OK
device /dev/md0 (/sw) is OK
device /dev/md2 (/state) is OK
device /dev/md6 (/local/local1/spool) is OK
device /dev/md5 (/local/local1) is OK
device /dev/md4 (/disk00-04) is OK
```

If any file system contains errors, the **disk_status.txt** file instructs you to repair it.

About RAID Synchronization and File System Errors

You must ensure that all RAID pairs are done rebuilding before you reboot your WAE device. If you reboot while the device is rebuilding, you risk corrupting the file system.

RAID pairs will rebuild on the next reboot after you enable WAAS core or edge services, use the **restore factory-default** command, replace or add a hard disk drive, delete disk partitions, or reinstall WAAS from the booted recovery CD-ROM.

To view the status of the drives and check if the RAID pairs are in “NORMAL OPERATION” or in “REBUILDING” status, use the **show disk details EXEC** command. When you see that RAID is rebuilding, you must let it complete that rebuild process. This rebuild process can take several hours.

If you do not wait for the RAID pairs to complete the rebuild process before you reboot the device, you may see the following symptoms indicating a problem:

- The device is offline in the Central Manager GUI.
- CMS can not be loaded.
- Error messages say that the file system is “read-only.”
- The syslog contains errors such as “Aborting journal on device md2,” “Journal commit I/O error,” “Journal has aborted,” and “ext3_readdir: bad entry in directory.”
- Other unusual behaviors related to disk operations or the inability to perform them.

If you encounter any of these symptoms, run the WAAS disk check tool to locate the problem. (For information about obtaining and using this tool, see the [“Running the WAAS Disk Check Tool”](#) section on page 3.)

Operating Considerations

This section includes operating considerations that apply to software version 4.0.9:

- [Using Full-Duplex Connections](#)
- [WAAS Print Driver Support and Interoperability](#)
- [WAAS Print Services CUPS Log Files](#)
- [Ensuring Subnets are Reachable using Static or Dynamic Routing Protocols](#)
- [Disabling the Automatic Machine Account Password Changes for the Edge WAE](#)
- [Using PortFast with Inline Mode](#)

Using Full-Duplex Connections

We strongly recommend that you do not use half-duplex connections on the WAE or on routers, switches, or other devices. Use of half-duplex impedes the system's ability to improve performance and should not be used. Double-check each Cisco WAE interface as well as the port configuration on the adjacent device (router, switch, firewall, WAE) to verify that full-duplex is configured.

WAAS Print Driver Support and Interoperability

WAAS WAE incorporates a Print Server based on the integration of open source Samba and CUPS technology. During the testing process, it has been determined that certain Print Drivers with complex features, such as sophisticated paper handling, may not be Point-and-Print compatible with WAAS. Most notably, Fiery Drivers incorporated into some Printer Manufacturer solutions are not compatible with Samba. Other Multi Function Printers (MFP) may also have limited functionality when working with Samba and are not supported by WAAS.

To determine if a Print Driver is compatible with WAAS, perform the Add Driver processes with a WAE using the Add Printer Wizard. Compare all the client Print features available after creating a print queue and compare it to a similar installation on a Microsoft Windows Print Server. If there are obvious feature inconsistencies, it is indicative of a Print Driver that cannot be used with WAAS Print Server for Point-and-Print. As a workaround, an installation on each client desktop from a CD or other source will be required.

When using the WAAS print services in a Windows XP Pro/Windows 2003 Server environment, you must register the WAE with Active Directory for the automatic printer driver download feature to operate correctly. This is due to a default computer policy for domain members that does not allow the host to download drivers from an unregistered device. A user will see a message similar to the following when encountering this issue: "A policy is in effect on your computer which prevents you from connecting to this print queue. Please contact your system administrator."

The WAAS print solution does not offer authentication. Any user may access and send print jobs to the WAAS print server. Also, WAAS supports 32-bit drivers.

WAAS Print Services CUPS Log Files

Common Unix Printing System (CUPS) log files are rotated when the log file reaches the maximum size of 1 MB.

Ensuring Subnets are Reachable using Static or Dynamic Routing Protocols

The Cisco WAAS provides transparent optimizations, which preserves source and destination IP addresses and TCP header information. Because of this, the Cisco WAE device must be deployed on separate subnets than those existing on the LAN, both on the server side and on the client side. These standalone subnets, and the Cisco WAE devices attached to them, must be reachable from the Central Manager and other WAE devices. Ensure that these subnets are reachable using static or dynamic routing protocols. If the subnets are not reachable, critical WAE functions may be impaired, including file protocol optimizations, WAE management, central management, and management authentication.

Disabling the Automatic Machine Account Password Changes for the Edge WAE

In a WAAS network where a Windows domain controller is configured for authentication and Disconnected Mode is enabled on an edge WAE, the domain controller authenticates content requests in the event of a WAN failure. By default, Windows domain controllers enforce automatic machine account password changes as part of the authentication process. The machine account password for the edge WAE is automatically negotiated and changed between the edge WAE and the domain controller every seven days. However, if the authentication service is down, this process may not occur, and the machine account password for the edge WAE may expire.

To prevent this situation, we recommend that you disable automatic machine account password changes for the edge WAE. The procedure that follows describes how to disable automatic machine account password changes for Windows XP and Windows Server 2003 using Group Policy Editor. Refer to Microsoft's Help and Support page for details on how to disable automatic machine account password changes for other Windows operating systems.

To disable the automatic machine account password changes for the edge WAE using Group Policy Editor, follow these steps:

-
- Step 1** On the domain controller, click **Start**, then choose **Run**.
 - Step 2** Enter **Gpedit** at the prompt, then click **OK**.
 - Step 3** Expand the Local Computer Policy, Windows Settings, Security Settings, Local Policies, Security Settings, Local Policies, Security Options.
 - Step 4** Configure the following setting: Domain Member: Disable machine account password changes (DisablePasswordChange).
-

Using PortFast with Inline Mode

When a WAE that has a Cisco WAE Inline Network Adapter installed enters bypass mode, the switch and router ports to which it is connected may have to reinitialize, and this may cause an interruption of several seconds in the traffic flow through the WAE.

If the WAE is deployed in a configuration where the creation of a loop is not possible (that is, if it is deployed in a standard fashion between a switch and a router), configure PortFast on the switch port to which the WAE is connected. PortFast allows the port to skip the first few stages of the Spanning Tree Algorithm (STA) and move more quickly into a packet forwarding mode.

Documentation Enhancements and Corrections

The following statement applies to the WAAS 4.0.9 document, *Cisco Wide Area Application Services Configuration Guide*, Chapter 4, “Configuring Traffic Interception”:

For traffic from the WAN to the LAN where the destination MAC address of the next hop is a multicast MAC address, the Cisco WAE Inline Network Adapter does not optimize the traffic. The Cisco WAE Inline Network Adapter optimizes traffic only if the next hop MAC address is a unicast address.

Software Version 4.0.9 Open and Resolved Caveats

The following sections list the open and resolved caveats for software version 4.0.9:

- [Software Version 4.0.9 Open Caveats](#)
- [Software Version 4.0.9 Resolved Caveats](#)

Software Version 4.0.9 Open Caveats

The following open caveats apply to software version 4.0.9:

- **CSCse71473**—After changing a local user’s password when the old password is a prefix of the new password, the user’s account encrypted password string is not changed. Additionally, only the first eight characters are used when setting a local account password.

- **CSCsg11506**—EPM (EndPoint Mapper)-based applications are unavailable in asymmetric routing scenarios. If the WAE receives packets going in one direction, but does not see packets returning from the other direction, the TFO handles this by establishing a pass-through. However, unlike the TFO, EPM always assumes that it will receive traffic going both directions and that the origin server is always up. EPM does not use autodiscovery. Instead, it terminates the 3-way handshake itself and establishes a new and separate spoofed TCP connection toward the server. Because of this behavior, if the server response bypasses the WAE (so that EPM does not intercept it), the client will receive a SYN+ACK for a TCP connection that it has already established and that has a different synchronization number. This situation causes the connection to be dropped. Workaround: Identify and resolve the cause of the asymmetric routing. If the cause of the asymmetric routing cannot be identified, or if a more immediate workaround is required, disable EPM. Acceleration will still be supported through the “Other” classifier. To disable EPM, enter the **no adapter epm enable** global configuration command from the CLI, or edit the device in the Central Manager GUI by de-selecting “EPM Classification” from the Device’s **Acceleration > Enable Features** window.
- **CSCsg79439**—DRE chunk aggregation can cause severe performance degradation as the same file is transferred over the WAN repeatedly over time. When very large files are transferred repeatedly over time, the disk cache becomes fragmented. Workaround: Clear the DRE cache.
- **CSCsh44391**—When using the Rsync, protocol a throughput drop is observed due to a large number of bytes bypassing the optimization module. This situation occurs when replicating a huge directory structure with hundreds of thousands of files using Rsync. Workaround: Increase the original TCP send/receive buffers to the maximum possible value (8 MB) as a partial work around. If the issue is still seen, break the transfer into multiple smaller transfers.
- **CSCsh47757**—A WAE reboots under heavy negative stress testing of HTTP traffic (200,000 connections for 14 hours).
- **CSCsh51624**—The Central Manager **Acceleration > Enabled Features** (previously General Settings) page will go to override mode. This can occur when the Blacklist Operation check box is unchecked and/or the Blacklist Server Address Hold Time is changed on this page in a device group, the device group is assigned to a WAE, and then the Central Manager is downgraded to a previous software version. Workaround: Click the Force Group Settings icon in the device group page to apply the device group settings to a WAE.
- **CSCsh69408**—The Central Manager sends updated configuration commands to a WAE for WCCP settings even when there is no change to the current running configuration. This situation occurs when a WCCP CLI change is made on a WAE that is managed by a Central Manager. This change is synchronized with the Central Manager, which then sends the change back to the WAE as CLI commands. The following commands are affected: **flow redirection, shutdown delay, slowstart, wccp router-list, and wccp version.**
- **CSCsh72271**—The transfer time for large files and multiple files that contain the same data becomes very slow over time, even if you have disabled chunk aggregation (level0 chunks only). By clearing the DRE cache, transfer times are restored to expected levels.
- **CSCsh76260**—Preposition fails after a file is successfully prepositioned, changed on the file server, and then the preposition task is run again after a few minutes.
- **CSCsh81163**—The last WAE in a WCCP farm redirects packets to another WAE (by flow-redirect) even though the other WAE does not own those buckets. These packets are dropped because of bad buckets. This situation occurs under heavy TCP traffic load with a Catalyst 6500 series switch, L2-redirect, mask-assign, flow-redirect, and no slow-start. Workaround: Disable flow-redirect.
- **CSCsh82935**—WAFS is locally failing write requests on files opened using an OpenPrintFile request. The open is successful and a FID is returned, but the write request that follows to that FID fails with STATUS_INVALID_HANDLE. OpenPrintFile requests are not supported.

- **CSCsh83544**—A login to the device manager GUI fails without any error message, regardless of the username or password used. This problem occurs when a managed component (such as an edge or core appliance) contains a Size object with a negative value in its data. (The Size object is used to store file sizes in bytes.) Workaround: Remove the negative Size value. If the Size value is in the preposition status data, remove the negative value by restarting the appliance. Preposition status data is removed from memory when the appliance is restarted.
- **CSCsh90244**—When you send a request for a web page from a Windows client (XP or Win2K) browser and the request goes through the WAE to a server that does not support Options in the SYN packet, the page is not displayed and an error message is returned. Workaround: Increase the number of SYN retransmissions in the Windows client to a minimum of three by adding or changing the HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\TcpMaxConnectRetransmissions value in the Windows registry. (For more information, see <http://support.microsoft.com/kb/120642>.)
- **CSCsi33808**—After a WAAS Central Manager database backup is restored, a WAE device reports that the current WAAS Central Manager activation timestamp is older than expected, so configuration changes are not propagated to the WAE device. Workaround: Follow these steps:
 - a. Ensure the WAAS Central Manager has the correct time.
 - b. Execute the following CLI commands on the WAAS Central Manager:


```
CentralManager# configure
CentralManager(config)# central-manager role primary
CentralManager(config)# cms enable
```
 - c. From the WAAS Central Manager GUI, trigger full resynchronization of registered devices by choosing **Devices > Device Groups**, selecting the AllDevicesGroup, and in the AllDevicesGroup home page, click the **Force full database update** icon in the toolbar.
- **CSCsi41577**—The NME-WAE module loses its IP address when the service module IP address is changed from the router. This problem occurs when the NME-WAE module is registered to a CM. Workaround: Reconfigure the module IP address, as follows:
 - a. Disable CMS on the NME-WAE by entering the **no cms enable** WAAS global configuration command.
 - b. Reconfigure the service module IP address from the router.
 - c. Enable CMS on the NME-WAE by entering the **cms enable** WAAS global configuration command.
- **CSCsi44406**—The WCCP slow-start option is automatically enabled when the WAE is registered to the Central Manager. Workaround: Disable the slow-start option from the Central manager GUI after the device is registered.

Software Version 4.0.9 Resolved Caveats

The following caveats were resolved in software version 4.0.9:

- **CSCsg24304**—Flow protection may stop working and active connections may hang or be reset when new WAEs are added to the WCCP cache farm.
- **CSCsh95484**—Numerous autodiscovery attempts to nonexistent servers causes socket leaks.

- **CSCsh96790**—The WAE-7326 is offline in the CM, is not responsive to ping, Telnet, or console commands, and requires a hard reboot.
- **CSCsi01081**—The syslog displays constant LZ buffer allocation failure messages, and the **show tfo connection summary** command displays Malloc failure messages.
- **CSCsi03647**—WAFS policies are not created properly when you upgrade from 4.0.5 to 4.0.7.
- **CSCsi03663**—The **match dst port eq 445** configuration is removed from the CIFS classifier when you upgrade the device to 4.0.7 and leave the CM in the lower version or when you upgrade the CM from a lower version to 4.0.7.
- **CSCsi07846**—The WAE hangs when it receives a malformed packet with a TCP header size that is less than 20 bytes.
- **CSCsi08294**—The CIFS pass-through connection is disconnected.
- **CSCsi13838**—The WAAS syslog contains maximum fanout exceeded messages.
- **CSCsi15758**—The EPM adaptor needs to be disabled by default in 4.0.9. If the EPM adaptor is enabled in a previous release and is upgraded to WAAS 4.0.9, the upgrade process should automatically set the EPM adaptor to disabled.
- **CSCsi16091**—When the WAE has been configured with an NTP server, and the server responds with a time value that is in the past from WAE current time, all the optimized connections through the WAE appear to hang, and the number of pending connections in the **show statistics tfo** display keeps increasing.
- **CSCsi22290**—When multiple clients are trying to access the same set of files concurrently, they receive an error message indicating that a file cannot be opened since it is being used by another program.
- **CSCsi24124**—After a reboot, the inline interface loses its speed (bandwidth) and duplex settings.
- **CSCsi28098**—The error log does not give a clear explanation for fanout errors, and the severity level for these errors is incorrect.

WAAS Documentation Set

In addition to this document, the WAAS documentation set includes the following publications:

- *Cisco Wide Area Application Services Quick Configuration Guide*
- *Cisco Wide Area Application Services Configuration Guide*
- *Cisco Wide Area Application Services Command Reference*
- *Cisco Wide Area Application Engine 511 and 611 Hardware Installation Guide*
- *Cisco Wide Area Application Engine 512 and 612 Hardware Installation Guide*
- *Cisco Wide Area Application Engine 7326 Hardware Installation Guide*
- *Cisco Wide Area Application Engine 7341, 7371, and 674 Hardware Installation Guide*
- *Cisco Network Modules Hardware Installation Guide*
- *Configuring Cisco WAAS Network Modules for Cisco Access Routers*
- *Installing the Cisco WAE Inline Network Adapter*
- *Regulatory Compliance and Safety Information for the Cisco Content Networking Product Series*

Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, submitting a service request, and gathering additional information, see the monthly *What's New in Cisco Product Documentation*, which also lists all new and revised Cisco technical documentation, at:

<http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html>

Subscribe to the *What's New in Cisco Product Documentation* as a Really Simple Syndication (RSS) feed and set content to be delivered directly to your desktop using a reader application. The RSS feeds are a free service and Cisco currently supports RSS version 2.0.

CCDE, CCENT, Cisco Eos, Cisco Lumin, Cisco StadiumVision, the Cisco logo, DCE, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn is a service mark; and Access Registrar, Aironet, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, CCVP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, EtherFast, EtherSwitch, Event Center, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, iQuick Study, IronPort, the IronPort logo, LightStream, Linksys, MediaTone, MeetingPlace, MGX, Networkers, Networking Academy, Network Registrar, PCNow, PIX, PowerPanels, ProConnect, ScriptShare, SenderBase, SMARTnet, Spectrum Expert, StackWise, The Fastest Way to Increase Your Internet Quotient, TransPath, WebEx, and the WebEx logo 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. (0804R)

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

© 2007-2008 Cisco Systems, Inc. All rights reserved.

