



Release Note for Cisco Wide Area Application Services

July 17, 2009



Note

The most current Cisco documentation for released products is also available on cisco.com.

Contents

This release note applies to Cisco Wide Area Application Services (WAAS) software version 4.0.13.23. 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.



Note

This release replaces and obsoletes WAAS software version 4.0.13.12. Customers that were previously using WAAS software version 4.0.13.12 with the WAE-612 must upgrade to WAAS software version 4.0.13.23 to take advantage of a disk driver upgrade (see resolved caveat [CSCsk03273](#)).

Software release 4.0.13.23 is the minimum release required to support the WAE-7341 and WAE-7371.

This release note contains the following sections:

- [WAAS Product Overview](#)
- [New Features for Software Version 4.0.13](#)
- [New and Changed Commands](#)
- [New Wide Area Application Engines Supported](#)
- [Changed Behavior for CIFS Connection Handling](#)
- [Upgrading From WAFS to WAAS](#)
- [Upgrading from a Prerelease Version to Version 4.0.13](#)
- [Upgrading from Version 4.0.x to 4.0.13](#)
- [Downgrading from Version 4.0.13 to a Previous Version](#)



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

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

- [Cisco WAE-674, WAE-7341, and WAE-7371 RAID Controller Firmware Upgrade](#)
- [Cisco WAE-612 Hard Disk Drive Replacement Notification](#)
- [Operating Considerations](#)
- [Documentation Enhancements and Corrections](#)
- [Open and Resolved Caveats](#)
- [WAAS Documentation Set](#)
- [Obtaining Documentation and Submitting a Service Request](#)

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 to 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 may use the WAAS Central Manager GUI to centrally configure and monitor the WAEs and application policies in your network. You may also use the WAAS Central Manager GUI to create new application policies so that the WAAS system will 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)

New Features for Software Version 4.0.13

WAAS software version 4.0.13 includes the following new features and changes:

- Supports FIPS 140-2 level 2 compliant 256-bit AES disk encryption with automatic and centralized key management to protect data in branch sites. This feature addresses the need to securely protect sensitive information that flows through deployed WAAS systems and that is stored in WAAS persistent storage. Disk encryption is supported as part of the WAAS Enterprise software license.

- Supports stateful firewall protection and virus scanning of accelerated data through fully tested interoperability with a wide range of Cisco IOS firewalls and security devices (such as, ASA, PIX, FWSM, IPS). WAAS interoperability is supported in Cisco IOS version 12.4(11)T2. To enable WAAS interoperability in the IOS firewall, use the IOS CLI command **ip inspect WAAS enable** (this command is disabled by default). WAAS interoperability is supported only when using WCCP redirection with the GRE packet forwarding method (not when using WCCP Layer 2 redirection).
Previous to IOS version 12.4(11)T2, the IOS firewall would drop packets that were being optimized by a WAAS device because WAAS increases the TCP packet sequence number during the TCP handshake. This behavior was viewed as a possible attack by the IOS firewall.
- Provides certified interoperability with NetQoS ReporterAnalyzer and SuperAgent version 7.2 (or later). The TCP Flow Agent for NetQoS integration is supported as part of the WAAS Enterprise software license.
- Supports configuring the egress method for WCCP interception mode. WCCP interception mode now supports two egress configuration options: IP forwarding and negotiated return. Negotiated return supports WCCP GRE as the WCCP egress method.
- Includes WAAS Central Manager enhancements that provide better reporting and graphic display of WAN optimization and performance. In addition, some monitoring and statistics pages have been renamed or relocated for easier access, as follows:
 - The CPU Utilization Report window in the Central Manager GUI has been moved from **Devices > Acceleration > Statistics > CPU Utilization** to **Devices > Monitoring > CPU Statistics**.
 - The Application Traffic Statistics Report windows in the Central Manager GUI have been moved from **Devices > Acceleration > Statistics** to **Devices > Monitoring > Optimization Statistics** (and **Optimization Statistics Details**).
 - The WAFS monitoring section in the Central Manager GUI (**Devices > Monitoring > WAFS**) has been renamed, CIFS Statistics.
- Provides the ability to monitor physical and logical disk information from the WAAS Central Manager. The Device Home window contains new fields that show the number of local disks and the RAID level. You may obtain further disk information details by viewing the new Disk Information for device window (**Devices > Devices > Monitoring > Disks**).
- Provides the ability to choose multiple directory roots (folders, shares) to preposition CIFS files from a single filer.
- Supports the new WAE-7341 and WAE-7371 appliances. For more information, see the section [“New Wide Area Application Engines Supported”](#) section on page 7.
- Supports hot swap functionality for WAE-612 and WAE-7326 hard disk drives. Supports hot-swapping of the WAE-7341 and WAE-7371 hard disk drives after the failed drive is properly shut down. (For the disk removal and replacement procedures for RAID-1 and RAID-5 systems, see the *Cisco Wide Area Application Services Configuration Guide*, Chapter 14.)
- Upgrades the database service code that is used on both WAAS Central Manager and WAE devices. The new database service code version fixes performance and data corruption issues. Version compatibility limitations affect software upgrade, rollback, downgrade, and Central Manager database backup and restore operations. For more information, see the section [“Central Manager Database Service Code Version Upgrade”](#) section on page 4.

Central Manager Database Service Code Version Upgrade

The WAAS 4.0.13 release includes an upgrade to the database service code that is used on both Central Manager and WAE devices. The new database service code version fixes performance and data corruption issues.

The database and backup files that are created by the new database service code version are not compatible with older database service code versions. Version compatibility limitations affect software upgrade, rollback, downgrade, and Central Manager database backup and restore operations. The database service code upgrade does not affect device printing configurations or the interoperability of Central Manager and WAE devices.

The database version upgrade in WAAS 4.0.13 affects WAAS version compatibility, as follows:

- Upgrade
 - Upgrades from pre-4.0.13 versions to WAAS 4.0.13 are fully automated for Central Manager and WAE devices.
 - Upgrade procedure preserves old database content that is used later for rollback operations.
- Rollback
 - Rollback from 4.0.13 to a previously installed pre-4.0.13 image is fully automated for Central Manager and WAE devices.
 - During rollback, the software restores the preserved pre-4.0.13 database files. All configuration changes made in WAAS 4.0.13 before the rollback will be lost. (Rollback is performed by using the **copy ... install** or the **restore rollback EXEC** commands.)
 - The rollback procedure for Central Manager devices requires that you re-synchronize your devices with Central Manager.

To re-synchronize all registered WAE devices with Central Manager, choose **Devices > Device Groups > AllDeviceGroup** from the Central Manager GUI, and click the **Force full database update** icon in the task bar.

If you use the **restore factory-default** command or if you repartition the disks, the preserved pre-4.0.13 database content will be erased. We strongly recommend that you perform a CMS database backup on the Central Manager before you perform either of these actions.
- Downgrade
 - Downgrade to a pre-4.0.13 image on a Central Manager or WAE device that was manufactured with the 4.0.13 image is not supported. Performing such a downgrade will cause database and management service failure. All configuration changes made in WAAS 4.0.13 before the downgrade will be lost.
 - Downgrade to a pre-4.0.13 image on a Central Manager or WAE device for which you have issued the **restore factory-default** command is not supported. Performing such a downgrade will cause database and management service failure. All configuration changes made in WAAS 4.0.13 before the downgrade will be lost.
 - Downgrade to a pre-4.0.13 image requires you to perform some manual configuration steps in the CLI.
- Central Manager Database Backup and Restore
 - The Central Manager database backup process is backward compatible only. It is not forward compatible.
 - WAAS 4.0.13 software can restore the pre-4.0.13 Central Manager database backup that was created by the pre-4.0.13 software.

- The pre-4.0.13 software cannot restore the WAAS 4.0.13 or later Central Manager database backup.

Wide Area File Services Database Upgrade

The WAAS 4.0.13 release includes an upgrade of the Wide Area Files Services (WAFS) database. Version compatibility limitations may affect software rollback and downgrade operations.

We recommend that you backup your WAFS configuration to a file before you perform any upgrade. You will then be able to restore this configuration if a downgrade becomes necessary. You must perform this backup for each device individually.

To backup and restore your WAFS configuration after a downgrade, follow these steps:

-
- Step 1** Back up your current WAFS configuration to a file by using the **wafs backup-config** *file_name* EXEC command.
- ```
WAE# wafs backup-config ConfigFile.tar.gz
```
- Step 2** Install the downgrade version of software. (See the [“Downgrading from Version 4.0.13 to a Previous Version”](#) section on page 13.)
- Step 3** Restore the WAFS configuration for this version by using the **wafs restore-config** *file\_name* EXEC command.
- ```
WAE# wafs restore-config ConfigFile.tar.gz
```
- Step 4** Clear the WAFS cache.
- From the gateway device GUI, choose **Cisco WAE > Utilities > WAFS Cache Cleanup**.
 - Follow the instructions in Help to stop the WAFS Edge service.
 - From the WAFS Cache Cleanup window, click **Run** to erase the contents of the cache.
-

New and Changed Commands

[Table 1](#) lists the new commands and command options that have been added in WAAS software version 4.0.13. (For more information, see the *Cisco Wide Area Application Services Command Reference*.)

Table 1 CLI Commands Added in Version 4.0.13

Mode	Command and Syntax
EXEC	cifs { auto-discovery { disable enable reset-log } mss <i>value</i> restart [core edge] reverse-dns { active enable disable } session disconnect [client-ip <i>ipaddress</i> server-ip <i>ipaddress</i>]}
	clear arp-cache [<i>ipaddress</i> interface { GigabitEthernet <i>I-2/port</i> PortChannel <i>I-2</i> Standby <i>I-4</i> }]
	clear statistics flow monitor tcpstat-v1
	debug flow monitor tcpstat-v1
	debug key-manager
	debug tfo connection egress-method [<i>acl</i>]
	disk insert <i>diskxx</i>
	disk disk-name <i>diskxx</i> replace (added in WAE-7341 and WAE-7371 only)
	disk recreate-raid (added in WAE-7341 and WAE-7371 only)
	show cifs { auto-discovery [enabled host-db last] cache { disk-use entry-count } connectivity peers mss requests { count waiting } sessions { count list }}
	show disks failed-disk-id (does not apply to WAE-7341 and WAE-7371)
	show disks tech-support
	show egress-methods
	show key-manager key
	show key-manager status
	show statistics cifs { cache eviction requests }
	show statistics flow { filters monitor tcpstat-v1 }
	show statistics key-manager
	show tfo egress-methods connection [local-ip <i>host-address</i> local-port <i>port</i> remote-ip <i>host-address</i> remote-port <i>port</i>]
	undebg key-manager
undebg tfo connection egress-method [<i>acl</i>]	
Global configuration	disk disk-name <i>diskxx</i> shutdown [force] (does not apply to WAE-7341 and WAE-7371)
	disk encrypt { enable disable }
	egress-method { ip-forwarding negotiated-return } intercept-method wcep
	flow monitor tcpstat-v1 { enable host <i>ip_address</i> }
	ip host <i>hostname ip-address</i>

Table 2 lists existing commands that have been modified in WAAS version 4.0.13.

Table 2 CLI Commands Modified in Version 4.0.13

Mode	Command and Syntax	Description
EXEC	show cdp neighbor	Displays inline port connections.
	show disks details	Supports the hardware RAID-5 configuration and displays the hardware RAID status.
	show running-config	Displays the non-default settings of the intercept-method global configuration command.
	show start-up config	Displays the non-default settings of the intercept-method global configuration command.
	show statistics wccp gre	Includes the following new counter: GRE packets sent to router (not bypass)
	show tech-support	Includes the output of the show tfo egress method command.
	show wccp gre	Includes the following new counter: GRE packets sent to router (not bypass)
Global configuration	interface InlineGroup <i>slot/grpnumber</i> [autosense bandwidth { 10 100 1000 } failover timeout { 1 3 5 } full-duplex half-duplex inline [vlan { all native <i>vlan_list</i> }] shutdown]	Includes speed and mode of operation options.

Table 3 lists commands that have been removed in WAAS version 4.0.13.

Table 3 CLI Commands Removed in Version 4.0.13

Mode	Command and Syntax
EXEC	disk mark
	disk reformat (removed in WAE-611 and WAE-7326 only)
	show disks smart-info
	show wccp modules
Global configuration	interface InlinePort
	wccp slow-start enable

New Wide Area Application Engines Supported

The WAAS 4.0.13 release introduces support for two new Wide Area Application Engine (WAE) appliances, the WAE-7341 and the WAE-7371. Similar in form and function to the WAE-7326 appliance, these next generation WAE appliances provide enhanced scalability, reliability, and performance, as described in the following sections:

- [Features and Benefits](#)
- [New and Changed Commands for the WAE-7341 and WAE-7371 Platforms](#)

Features and Benefits

The WAE-7341 and WAE-7371 appliances provide the following features and benefits:

Feature	Benefit
Hardware RAID-5	Allows the appliance to continue operating with one drive in a non-functioning state for increased reliability. Provides increased logical disk capacity.
Disk hot-swap capability	No downtime when removing or installing hard disk drives.
64-bit kernel	Allows a larger memory footprint for the TCP Proxy application and increases the number of concurrent optimized connections for increased scalability and performance.
300-GB SAS ¹ hard disk drives	4 x 300 GB in the WAE-7341 6 x 300 GB in the WAE-7371
Disk monitoring	Allows you to monitor, analyze, and control the RAID status through the CLI and view basic disk status in the RAID from the Central Manager GUI.

1. SAS = Serial Attached SCSI

New and Changed Commands for the WAE-7341 and WAE-7371 Platforms

Table 4 lists commands have been added in the WAAS 4.0.13 release to support the new WAE-7341 and WAE-7371 platforms. These commands apply to the WAE-7341 and WAE-7371 only.

Table 4 CLI Commands Added in Version 4.0.13 for WAE-7341 and WAE-7371

Mode	Command and Syntax	Description
EXEC	show disks tech-support	Displays all available information from the RAID controller, including disk status (logical and physical), disk vendor ID, and serial numbers. On other WAEs, this command replaces the show disk smart-info EXEC command.
	disk disk-name <i>diskxx</i> replace	Shuts down the disk for removal.
	disk recreate-raid	Removes the logical drive from the RAID-5 array and then recreates the RAID array. All data contained in the logical drive will be lost. The operation of this command results in synchronizing all drives. While the drives are synchronizing, the system remains operational, but the performance will be slower.
Global configuration	disk logical shutdown	Shuts down the RAID-5 array.

Table 5 lists existing commands that have been modified in the WAAS 4.0.13 release to support the new WAE-7341 and WAE-7371 platforms. These modifications apply to the WAE-7341 and WAE-7371 only.

Table 5 CLI Commands Modified in Version 4.0.13 for WAE-7341 and WAE-7371

EXEC	disk scan-errors	This command is now available on the logical drive for the WAE-7341 and WAE-7371. The syntax of the existing command has been modified for RAID-5 systems; the <i>diskname</i> option has been removed. The functionality remains the same.
	disk delete-partitions	This command is now available on the logical drive. This command deletes the entire logical RAID-5 volume. The syntax of the existing command has been modified for RAID-5 systems; the <i>diskname</i> option has been removed. The functionality remains the same. On the next reboot, if the RAID array is still identified as good, the partition table will be recreated and all partitions will be initialized, during which time, the system will not process any traffic.

Table 6 lists commands have been removed for the WAE-7341 and WAE-7371 in the WAAS 4.0.13 release. These commands are still available on other supported WAE hardware platforms.

Table 6 CLI Commands Removed in Version 4.0.13 for WAE-7341 and WAE-7371

Mode	Command and Syntax	Description
EXEC	show disks failed-sectors	Failed disk sectors are monitored internally by the RAID controller.

Changed Behavior for CIFS Connection Handling

In previous versions of WAAS, when the number of incoming and outgoing connections on CIFS ports 139 and 445 exceeded the connection limit, the WAFS Edge would reset the connection and block further connections. In WAAS 4.0.13, when the maximum number of optimized TCP connections is reached, further connections are no longer dropped or blocked, but are passed through using the default DRE/TFO optimization policy.

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.

Note the following points regarding upgrading from WAFS to WAAS:

- When you upgrade from WAFS to WAAS, up to half of the WAFS cache space may be lost. The upgrade process uses the WAFS cache eviction process to reclaim the space needed for the DRE cache; the oldest content is removed first.
- The hardware that supports WAFS 3.0 will also support WAAS, with the exception of the NM-CE.
- You will need a dedicated WAE to function as the Central Manager in WAAS.
- The WAEs will need to be placed in a separate subnet from the clients, or you will need to use the GRE return feature.

Upgrading from a Prerelease Version to Version 4.0.13

To upgrade from WAAS prerelease software to version 4.0.13, 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 4.0.13

This section contains the following topics:

- [Requirements and Guidelines](#)
- [Running the WAAS Disk Check Tool](#)
- [Ensuring RAID Pairs Rebuild Successfully](#)

Requirements and Guidelines

When you upgrade from version 4.0.x to version 4.0.13, 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 may result from a RAID synchronization failure. See the [“Running the WAAS Disk Check Tool”](#) section on page 11.
- Upgrade the WAE devices first, and then upgrade the WAE Central Manager devices.
- If you operate a network with devices that have different software versions, the WAAS Central Manager must be the lowest version.
- To ensure that all regularly scheduled preposition tasks relevant to a Core cluster will continue to operate as expected without any intervention, set the “Ignore hidden directories” flag on the Core cluster before you upgrade to 4.0.13. If you edit the preposition directive after the upgrade, reset the “Ignore hidden directories” flag to ensure that the same functionality is maintained.
- In WAAS 4.0.13 the **InlinePort** interface mode command has been removed. In releases prior to WAAS 4.0.13, the **InlinePort** command required you to configure autosense, bandwidth, and mode settings that were specific to LAN and WAN ports. In WAAS 4.0.13, these settings are now

configured for the InlineGroup interface and are common to all ports. When you upgrade the Central Manager to 4.0.13, the upgrade script uses the inlinePort LAN values to populate the inlineGroup autosense, bandwidth, and mode settings. Any values configured for the WAN port are ignored.

- When you upgrade the Central Manager to version 4.0.13, the CIFS-non-wafs classifier is removed from Edge and Core devices automatically. (This classifier was removed in version 4.0.7.)
- When you upgrade Edge and Core devices to version 4.0.13, 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 > Policy 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.
-

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 may result from a RAID synchronization failure. (For more information, see the “[Ensuring RAID Pairs Rebuild Successfully](#)” section on page 12.) 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 may obtain the WAAS disk check tool from the following URL:

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

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.

To run the WAAS disk check tool, follow these steps:

-
- Step 1** 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
```

- Step 2** 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: /local/1PAM_unix[26162]: ### pam_unix: pam_sm_close_session (su) session closed
```

```
for user root
waitpid returns error: No child processes
No child alive.
```

Step 3 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
```

Step 4 If a file system contains errors, follow the instructions in the `disk_status.txt` file to repair the file system.

Ensuring RAID Pairs Rebuild Successfully

RAID pairs will rebuild on the next reboot after you 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.

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.

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** command in EXEC mode. When you see that RAID is rebuilding, you must let it complete that rebuild process. This rebuild process may 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 cannot 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 11.)

Downgrading from Version 4.0.13 to a Previous Version

When you downgrade from version 4.0.13 to a previous version, observe the following compatibility issues:

- If you enable disk encryption and then downgrade to a software version that does not support this feature, you will not be able to use the data partitions. In such cases, you must delete the disk partitions after you downgrade.
- Before you downgrade from 4.0.13 to a previous version of WAAS, we strongly recommend that you save any user accounts that were added or changed in the 4.0.13 software to the startup-config by using the **write memory** command in EXEC mode.

Passwords in WAAS 4.0.13 are encrypted using an MD5 encryption algorithm, which results in the generation of a 34-byte encrypted password. If you add new users and create new passwords or make changes to existing passwords in WAAS 4.0.13 (or later), and then revert to an earlier software version where the DES encryption algorithm is used (generating a 13-byte encrypted password), all user accounts with 34-byte encrypted passwords will be lost unless you have saved them to the startup-config.

When the user password reverts to DES encryption as a result of the downgrade, the password is truncated to the first 8 characters if it is longer than 8 characters.

Admin accounts will revert to the default password.

- Because the Central Manager database has been upgraded in WAAS 4.0.13, we do not support a downgrade script for downgrading the Central Manager to a prior release. If you downgrade, you must restore the Central Manager database from a backup of the prior release. (See the “[Central Manager Database Backup and Restore](#)” section on page 4.)

To downgrade Central Manager and WAE devices to a pre-4.0.13 image, follow these steps:

-
- Step 1** Disable the management service by using the **no cms enable** global configuration command.
- ```
(config)# no cms enable
```
- Step 2** From the Central Manager CLI, create a database backup by using the **cms database backup** EXEC command.
- ```
CentralManager# cms database backup
```
- Step 3** Install the pre-4.0.13 image by using the **copy install** EXEC command.
- Step 4** Reload the device.
- Step 5** After the device reloads, enter the **cms database delete** EXEC command.
- ```
cms database delete
```
- This command deletes and re-initializes the internal database files and restarts the database service.
- Step 6** Initialize the CMS database tables by using the **cms database create** EXEC command.
- ```
# cms database create
```
- Step 7** On the Central Manager, restore the pre-4.0.13 CMS database backup, if available.
- ```
CentralManager# cms database restore <pre-4.0.13-db-backup>
```
- Step 8** Enable the CMS service by using the **cms enable** global configuration command.
- ```
(config)# cms enable
```
-

Cisco WAE-674, WAE-7341, and WAE-7371 RAID Controller Firmware Upgrade

Under rare circumstances, the RAID controller firmware used in the WAE-674, WAE-7341, and WAE-7371 appliances can cause the disk storage subsystem to go offline and the affected devices to stop optimizing connections. The symptoms are as follows:

- Syslog output contains several instances of the following message:
“WAAS-SYS-3-900000: sd 0:0:0:0: rejecting I/O to offline device.”
- A sysreport and running-config cannot be generated and copied to /local/local1.

Both of the above symptoms are an indication of the file system becoming read-only during traffic flow.

- An increasing number of pending connections appear in the output of the **show statistics tfo** command, indicating that new connections cannot be optimized. You can use this command to proactively check the functionality of the system.

The solution is to upgrade to the 5.2-0 (15427) RAID Controller Firmware, which can be found on cisco.com at the [Cisco Wide Area Application Engine \(WAE\) Utilities Software Downloads \(registered customers only\)](#) page. The firmware binary image is named L4_15427_FIRMWARE.bin.

Instructions on how to apply the firmware update are posted on cisco.com together with the firmware and are named L4_15427_FIRMWARE.pdf.

Cisco WAE-612 Hard Disk Drive Replacement Notification

This notice applies to the WAE-612 and all WAAS versions previous to 4.0.19 that support the hot-swap replacement of drives while the appliance is running.

A problem may occur when replacing the drives while the unit is running. Occasionally after a drive hot-swap procedure, the WAE-612 may stop operating and require a reboot.

To avoid this problem, upgrade your WAAS software to version 4.0.19 or later.

This notice does not apply to the WAE-674, WAE-7341, or WAE-7371.

Operating Considerations

This section includes operating considerations that apply to software version 4.0.13:

- [Using Autoregistration with PortChannel Interfaces](#)
- [Default Behaviors for EPM Classification](#)
- [WCCP Configuration](#)
- [WAFS Support of FAT32 File Servers](#)

Using Autoregistration with PortChannel Interfaces

Do not enable the **auto-register** global configuration command when both interfaces are configured as PortChannel interfaces.

Default Behaviors for EPM Classification

In WAAS 4.0.9, EndPoint Mapper (EPM) Classification (or EPM adaptor) is disabled by default in the WAE, but enabled by default in the Central Manager. Because of this discrepancy, EPM Classification that is disabled in version 4.0.7, becomes enabled after you upgrade to version 4.0.9 when the Central Manager sends database updates along with its default settings to the WAES in the network.

In WAAS 4.0.11 and 4.0.13, the default discrepancies between the WAES and the Central Manager have been corrected, and a new line in the code has been added to disable EPM Classification for the following scenarios:

- Newly manufactured WAAS 4.0.13 WAES and Central Managers after running the startup script
- Central Managers and WAES after an upgrade to 4.0.13
- WAES with EPM Classification enabled when registered to a 4.0.13 Central Manager
- Any WAAS 4.0.13 device on which the **restore factory defaults** command is used

To enable EPM Classification in 4.0.13, you must explicitly enable it after you upgrade to 4.0.13.

To enable EPM Classification, follow these steps:

-
- Step 1** From the Central Manager GUI, choose **Devices > Device Groups**.
- Step 2** Click the **Edit** icon next to the name of the device group for which you want to configure EPM Classification.
- Step 3** In the Contents pane, choose **Acceleration > Enabled Features**. The Enabled Features for Device Group window appears.
- Step 4** Check the EPM Classification check box, if not already checked.
- When a device group does not have any active settings configured, the check box for the EPM Classification option is checked by default. This setting is effective only when there is an active configuration.
- Step 5** To activate the device group settings and enable EPM Classification, click **Submit**.
- Step 6** To apply your device group settings to your devices, click the **Force Settings for All Devices in Group** icon in the taskbar.

This icon only appears in the taskbar when the EPM Classification check box is checked and the configuration is active.

WCCP Configuration

When using WCCP interception, the maximum throughput per WAAS interface should not exceed 800 Mbps. When using hardware-assisted WCCP switches or routers capable of Gigabit line-rate WCCP forwarding along with line-rate capable WAAS devices (WAE-7341 and WAE-7371), the recommended QoS and policy configuration should be applied on the WAAS-facing switch or router interfaces to ensure that the maximum throughput is not exceeded. When full Gigabit line-rate traffic optimization is required, it is recommended to use Cisco ACE or the WAAS device with inline interception module.

WAFS Support of FAT32 File Servers

The WAFS feature does not support file servers that use the FAT32 file system. You can use the policy engine rules to exclude any file servers that use the FAT32 file system.

Documentation Enhancements and Corrections

The following enhancements and corrections apply to the WAAS 4.0.13 documentation set.

- The following statement applies to the *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.

- The WCCP GRE return egress method of WCCP interception allows you to place WAEs on the same VLAN or subnet as clients and servers. Repeating redirection is prevented by encapsulating the outgoing frames in the GRE frames. IOS routers handle these GRE frames as bypass frames and do not apply WCCP redirection. WAAS uses the router ID address as the destination for GRE frames. This technique makes it possible to support redundant routers and router load balancing and return frames back to the router from which they arrived. If you want to use this functionality with multiple routers connected to the WAAS network segment, you need to ensure connectivity to the router ID address, for example, by configuring static routes.

The router ID is the address of the first loopback interface or highest active physical interface. This address can be found in the output of the **show wccp routers EXEC** command.

- The **ip host hostname ip-address** global configuration command was added in version 4.0.13. This command adds an entry to the `/etc/hosts` file on the device, mapping the specified hostname to the specified IP address. A given hostname can be mapped only to a single IP address, while an IP address can have multiple hostnames mapped to it, each one through a separate issuance of this command.

The command **no ip host hostname ip-address** removes the entry from the `/etc/hosts` file.

The **ip host** command operates on devices in either the application-accelerator or central-manager device mode. This command has no default behavior.

You can use the **show hosts EXEC** command to display the contents of the `/etc/hosts` file.

- The **external-ip** global configuration command is inadvertently documented in the *Cisco Wide Area Application Services Command Reference* but it is not part of the WAAS software.
- Any user account that has print admin privileges must also be assigned a domain, which defines the device groups or WAEs that are accessible by the user. All WAEs to which the user needs access should be members in the assigned domain.

To assign a domain to a user account, from the WAAS Central Manager GUI, choose **System > AAA > Users**. Click the **Edit** icon next to the user account for which you want to assign domains. Click the **Assign** icon (blue cross mark) that appears next to the domain name that you want to assign to the selected user account. To save the changes, click **Submit**.

- If a WAE is unable to reach the WAAS Central Manager during a boot, it will do everything except mount the encrypted partitions. In this state, all traffic will be handled as pass-through. Once communication with the WAAS Central Manager is restored (and the encryption key is obtained), the encrypted partitions are mounted. There is no loss of cache content.

- The WAAS print server page log is stored in `/local/local1/logs/cups_access_log`. The `cups_access_log` file lists each page that is sent to a printer. Each line contains the following information:

```
printer user job-id date-time page-number num-copies job-billing hostname
```

Here is an example of a log entry:

```
DeskJet root 2 [20/May/1999:19:21:05 +0000] 1 0 acme-123 localhost
```

The field descriptions are as follows:

- The *printer* field contains the name of the printer that printed the page. If you send a job to a printer class, this field will contain the name of the printer that was assigned the job.
 - The *user* field contains the name of the user (the IPP `requesting-user-name` attribute) that submitted this file for printing.
 - The *job-id* field contains the job number of the page being printed. Job numbers are reset to 1 whenever the CUPS server is started, so do not depend on this number being unique.
 - The *date-time* field contains the date and time of when the page started printing. The format of this field is identical to the *date-time* field in the `access_log` file.
 - The *page-number* and *num-pages* fields contain the page number and number of copies being printed of that page. For printers that cannot produce copies on their own, the *num-pages* field will always be 1.
 - The *job-billing* field contains a copy of the `job-billing` attribute provided with the IPP `create-job` or `print-job` requests or "-" if none was provided.
 - The *hostname* field contains the name of the host (the IPP `job-originating-host-name` attribute) that originated the print job.
- The last sentence in the section “[Calculating the TCP Buffers for High BDP Links](#)” in Chapter 12, “Configuring Application Acceleration,” in the *Cisco Wide Area Application Services Configuration Guide* should read as follows:

Once you calculate the size of the Max BDP, enter that value in the Send Buffer Size and Receive Buffer Size for the optimized connection on the Acceleration TCP Settings window.
 - Step 3 in the section “[Installing Print Drivers on Individual WAAS Print Servers](#)” in Chapter 13, “Configuring and Managing WAAS Print Services,” in the *Cisco Wide Area Application Services Configuration Guide* should read as follows:

View the printers configured in the WAAS Print Server by opening the Printers folder.
 - The note in Step 9e in the section “[Creating an Application Policy](#)” in Chapter 12, “Configuring Application Acceleration,” in the *Cisco Wide Area Application Services Configuration Guide* should read as follows:



Note To specify a range of IP addresses, enter a wildcard subnet mask in either the destination or source IP Wildcard field.

Open and Resolved Caveats

The following sections list the open and resolved caveats for software version 4.0.13:

- [Software Version 4.0.13 Open Caveats](#)
- [Software Version 4.0.13 Resolved Caveats](#)

Software Version 4.0.13 Open Caveats

The following open caveats apply to software version 4.0.13:

- **CSCsg11506**—EndPoint Mapper (EPM)-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 in both directions and that the origin server is always active. 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** command in global configuration mode from the CLI, or edit the device in the Central Manager GUI by unchecking the EPM Classification check box from the Device **Acceleration > Enable Features** window.
- **CSCsh93105**—When both Edge and Core WAEs are configured to use WCCP L2 redirect and IP forwarding as the egress method (IP forwarding is the default), they continue to use an MSS value of 1432 even though it is possible to use 1460. Changing the MSS value to 1460 by using the **tfo tcp optimized-mss 1460** or **tfo tcp original-mss 1460** global configuration commands does not work, and the WAEs continue to use an MSS value of 1432. Workaround: None.
- **CSCsi10702**—When you replace the Central Manager either by performing a backup and restore of the Central Manager database or by adding a standby Central Manager, the print drivers are not backed up or passed to the standby Central Manager. Workaround: Manually copy the print drivers from the primary Central Manager to the standby Central Manager.
- **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 that the WAAS Central Manager has the correct time.
 - b. From the WAAS Central Manager CLI, enter the following sequence of commands:


```
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: choose **Devices > Device Groups > AllDevicesGroup** and click the **Force full database update** icon in the toolbar.
- **CSCsi66278**—When you access a fileshare on the DFS root of a NetApp filer, you may see the following error message: NT_STATUS_NO_SUCH_FILE. Workaround: Remove the DFS root file server from the optimized servers configuration of WAAS.
- **CSCsj16259**—When you copy a file that is larger than 10 MB from the server and the file is not in the CIFS file cache, or the DRE cache does not contain references to part of this file, the copy status bar freezes for 10 to 20 seconds during the transfer. This problem occurs on high-bandwidth and high-latency links. Workaround: Reduce the maxReadAheadSize value from 5 Mb to 2.5 Mb in Rx expert mode. This workaround improves the freeze time, but the total copy time remains the same.

To reduce the maxReadAheadSize value, follow these steps:

- a. Enter Edge WAE expert mode.

- b. Choose **Rx > RxServer 3**.
- c. Find the field, “readAheadMaxSize” and change its value to **4**.
- d. Add the string, “readAheadMaxSize” into NetworkConfigurationLocalEntries.
- e. Save the modification.

If WAN settings will be significantly lower in the future (for example, reduced from T3/200ms to T1/80ms), remove the “readAheadMaxSize” string from NetworkConfigurationLocalEntries to allow the proper read-ahead calculation.

- **CSCsj32479**—NTLM authentication fails when the AUTH3 method is used on the server with EPM Classification enabled on the WAE. Workaround: Use another classification method. For example, create an application with a classifier based on the server IP address and add it to the bottom of the prioritized policy list.
- **CSCsj43783**—WAFS CIFS statistics pie chart is blank, even though an alias has been successfully configured, acceleration is occurring, and you are able to browse shares using the alias created for the configured server.
- **CSCsj69884**—When a WAE is configured using the Standby Interface feature, DHCP discovery requests continue to be generated even when a static IP address is configured. Workaround: None.
- **CSCsj75713**—CUPS services are not available on the WAE-7341 or WAE-7371. When you add a new printer to the WAE, you may receive the following error message:
server-error-service-unavailable. Workaround: None.
- **CSCsj80333**—When you transfer files to a CIFS share with a MAC client running MAC OS version 10.4.10, all of the MAC clients receive a “Finder Error-36” when they attempt to push the file. The highest MAC OS version that WAAS supports is MAC OS version 10.3.9. Workaround: None.
- **CSCsj99291**—A core dump occurs in the Edge core_dir/ when you configure trusted domains and register the device to the Domain Controller using NTLM.
- **CSCsj99810**—Prepositioning tasks end with an error message when the first root directory defined does not exist on the file server. The other directories are not prepositioned either. Workaround: Remove the first root directory defined in the Preposition page of the Central Manager and restart the preposition task.
- **CSCsj99861**—When you preposition files from a directory on the FAT32 partition using a Windows 2003 server, the status of the preposition task remains InProgress, and no files are copied from the Core WAE to the Edge WAE. This problem does not occur with the NTFS partition. Workaround: None.
- **CSCsk41815**—The /local/local1 (SYSFS) partition runs out of space when TFO transaction logging is enabled and there is a lot of traffic going through the box. TFO transaction logs are normally removed after two days, but if many connections occur in one day, they can fill up the disk. Workaround: Either disable the TFO transaction logging or remove the log files manually.
- **CSCsm50810**—Occasionally, the WAE-612-K9 may reboot automatically or enter KDB mode and hang when you perform a hard drive hot replacement using the following procedure:
 - a. Enter the **disk disk-name disk00 shutdown** command.
 - b. Remove one hard drive and insert a new drive onto disk00.

After performing the above hard drive replacement procedure with any set of supported Cisco hard drives of the same capacity (regardless of RPM speed) for the WAE-612, in some instances the WAE-612-K9 may reboot automatically or enter KDB mode and hang.

Workarounds: Perform one of the following:

- Upgrade to WAAS version 4.0.19 or later, in which the problem is fixed, before performing the hot swap procedure.
- Perform a cold-swap procedure by first powering down the WAE-612 before swapping the drives.
- If you do not upgrade to WAAS version 4.0.19 or later and the device hangs, power cycle the WAE-612-K9.

**Note**

See [“Cisco WAE-612 Hard Disk Drive Replacement Notification”](#) for the notice that applies to the WAE-612 and all WAAS versions that support the hot-swap replacement of drives while the appliance is running.

Software Version 4.0.13 Resolved Caveats

The following caveats were resolved in software version 4.0.13:

- **CSCsg79439**—DRE chunk aggregation may cause severe performance degradation because the same file is transferred over the WAN repeatedly over time.
- **CSCsh44391**—When the RSYNC protocol is used, a throughput drop is observed as packets bypass the optimization module.
- **CSCsh51624**—The Central Manager **Acceleration > Enabled Features** (previously General Settings) page goes into override mode.
- **CSCsh72271**—DRE file transfers become slow for files that are repeatedly transferred over several weeks.
- **CSCsh82935**—WAFS is locally failing write requests for files opened using an OpenPrintFile request.
- **CSCsi40052**—The sshd process crashes on the WAAS Central Manager.
- **CSCsi41790**—An alarm may not be raised on the Central Manager when the WAFS service is stopped on the WAE.
- **CSCsi42714**—The Central Manager device does not support an inline card.
- **CSCsi53659**—Clicking the Submit button in the preposition directive configuration window causes a full scan for the preposition directive, even though the content of the preposition directive has not been modified.
- **CSCsi54867**—The configuration from the Central Manager is not applied to the WAE startup-config.
- **CSCsi58271**—The CIFS Cache Hit Rate graphs on the Edge WAE are not reflecting the correct hit rate.
- **CSCsi65531**—CIFS requests should be automatically excluded from the CIFS Active Directory in connected WAFS Core devices.
- **CSCsi69388**—The NME-WAE configured static IP routes that are associated in the routing table appear incorrectly, and the management connectivity is lost.
- **CSCsi72542**—When two or more clients are using MS Remote Installation Services (RIS) on a Windows 2000 server, the clients receive a blue screen and hang.
- **CSCsi80547**—WAAS prepositioning jobs are always scheduled at UTC time and not at the local WAE time.

- **CSCsi82465**—SNMP crashes in the initialization phase.
- **CSCsi88461**—The IP ACL counter for the SNMP server is always zero regardless of the number of matches that have occurred.
- **CSCsi88518**—Prepositioned content is ignored, and a CIFS cache miss occurs when a request is made by a NETBIOS client.
- **CSCsi90785**—An Edge WAE in inline mode with over 1500 static CIFS connections and 700 dynamic CIFS clients running entered KDB mode after two hours.
- **CSCsi94666**—After two hours of operation, the NM-WAE-502 generates a core file related to SNMP.
- **CSCsi95089**—When EPM classification is enabled on one Edge device and not at the Core, the syslog fills with kernel messages.
- **CSCsi96571**—Fifty percent of Edge devices failed to automatically reconnect to a Core that was taken out of service for maintenance.
- **CSCsi98147**—When local print services are configured, users and printadmin users cannot modify or delete jobs from the Print Services Administration GUI.
- **CSCsj13021**—The CLI error log truncates the commands that were issued so you cannot determine the exact command that was issued.
- **CSCsj13211**—A client cannot access files under a directory for which Dynamic Shares is enabled.
- **CSCsj17029**—On the initial connection from a client to a server that is being optimized using WAAS, if the client sends its first ACK to the server with a window size equal to zero, the connection fails.
- **CSCsj20743**—The WAE does not clear the existing connection, so a client cannot mount the home directory.
- **CSCsj27886**—If you modify the **wccp tcp-promiscuous mask** command value from the WAE command line interface, the mask is changed successfully. But when you view the WCCP service configuration from the Central Manager GUI, both the old service mask configuration and the new service mask configuration are displayed.
- **CSCsj35368**—Kerberos authentication fails after you reload the WAAS NME-WAE.
- **CSCsj37129**—The client fails to redirect to the Web filter authentication page, breaking all HTTP communications to the Internet.
- **CSCsj61292**— After restoring the Central Manager database, the CMS status of all devices registered with the Central Manager remains Offline.
- **CSCsj65486**—When the WAE-7341 or WAE-7371 appliances reboot, the software recreates the partitions and reinitializes the filesystem. The WAE displays filesystem (EXT3) errors, and the software remounts the filesystem in read-only mode.
- **CSCsj96882**—When auto-registration was enabled in a WAE-612 with port channel 2 configured, the WAE entered KDB mode.
- **CSCsk02612**—The WCCP Services Mask values are removed when you override the device group configurations from the CLI.
- **CSCsk03273**—WAE-612 devices experience hard disk drive failures after being upgraded to release 4.0.13-b12.
- **CSCsk15029**—Tcproxy continuously crashes when disk encryption is enabled, which failed to initialize due to various issues.

- **CSCsk29503**—The WCCP Service settings are removed after performing a series of configuration steps.
- **CSCsk30813**—DRE “sub hash table full” error messages flood the syslog. There is a large number of “Index table full events” shown in the output of the **show statistics dre detail** command.

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, CCSI, Cisco Eos, Cisco HealthPresence, Cisco Ironport, the Cisco logo, Cisco Lumin, Cisco Nexus, Cisco Nurse Connect, Cisco Stackpower, Cisco StadiumVision, Cisco TelePresence, Cisco Unified Computing System, Cisco WebEx, DCE, Flip Channels, Flip for Good, Flip Mino, Flip Video, Flip Video (Design), Flipshare (Design), Flip Ultra, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn, Cisco Store, and Flip Gift Card are service marks; 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, iQuick Study, IronPort, the IronPort logo, LightStream, Linksys, MediaTone, MeetingPlace, MeetingPlace Chime Sound, 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. (0907R)

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.

