



Release Note for Cisco Wide Area Application Services

WAAS Version 4.0.7
May 6, 2008



Note

The most current Cisco documentation for released products is also available on 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 4.0.7. 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](#)
- [Important Note About the EPM Classification Feature](#)
- [New Features for Software Version 4.0.7](#)
- [New and Changed Commands](#)
- [Upgrading From WAFS to WAAS](#)
- [Upgrading from a Prerelease Version to Version 4.0.7](#)
- [Upgrading from Version 4.0.x to 4.0.7](#)
- [Operating Considerations](#)
- [Documentation Correction](#)
- [Software Version 4.0.7 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)

Important Note About the EPM Classification Feature

Because of a known issue with the global optimization EPM Classification feature, EPM traffic in asymmetric routing environments causes connections to be dropped between clients and servers for applications such as, Microsoft Exchange, Active Directory, and others. (For more information about this issue, see CSCsg11506 in the [“Software Version 4.0.7 Open Caveats” section on page 14.](#))

The WAAS 4.0.7 release enables the EPM Classification feature by default. If you are supporting an environment with asymmetric routing, you must manually disable the EPM Classification feature on all WAEs in the network through the Central Manager.

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. (For more information, see the *Cisco Wide Area Application Services Configuration Guide*, Software Version 4.0.7.)

New Features for Software Version 4.0.7

WAAS software version 4.0.7 includes the following new features and changes:

- Support for intercepting traffic directly by using a new inline mode with a WAE that has a Cisco WAE Inline Network Adapter installed.
- Support for enabling or disabling inline mode for specific VLANs.
- Support for automatic discovery of CIFS file servers in the WAFS service. With the automatic discovery feature, WAAS will attempt to automatically discover and connect to a new file server when a transparent mode CIFS request is received. If there are multiple paths to the file server, WAAS chooses the path with the lowest latency. If the latency between the core WAE and the discovered server is more than 25 milliseconds, the server is considered to be too far away, and the connection will not be optimized. Additionally, if the latency between the edge WAE and the server is less than 2 milliseconds, the server is considered to be local, and the connection will not be optimized.
- Support for better handling of situations in which TCP setup packets that have options are blocked or not returned to the WAE device. This behavior can result from network devices (such as firewalls) that block TCP setup packets that have options and from asymmetric routes. WAAS now keeps track of origin servers (such as those behind firewalls) that cannot receive optioned TCP packets and learns not to send out TCP packets with options to these blacklisted servers. WAAS is still able to accelerate traffic between edge and core WAEs in situations where optioned TCP packets are dropped.
- Removal of WCCP Version 2 CIFS caching service (service 89) and corresponding service masks. This feature is no longer needed because WCCP Version 2 TCP promiscuous mode service provides the same functionality.
- The WAAS Central Manager screen for Windows Domain Settings has been changed to remove the check boxes that enabled Windows domain authentication. After you use this screen to configure Windows domain settings, you must set Windows as the authentication and authorization method for the device by using the Authentication Methods screen. The Disconnected Mode check box was also moved to the Authentication Methods screen.

New and Changed Commands

[Table 1](#) lists the new commands and command options that have been added in WAAS software version 4.0.7. (For more information, see the *Cisco Wide Area Application Services Command Reference*.)

Table 1 CLI Commands Added in Version 4.0.7

| Mode | Command and Syntax | Description |
|----------------------|---|--|
| EXEC | clear statistics inline | Clears the inline interception statistics. |
| | clear statistics tfo blacklist | Clears the TFO blacklist statistics. |
| | debug tfo synq | Enables TFO connection debugging for the SynQ module. |
| | show adapter epm | Displays the status and configuration of the EndPoint Mapper (EPM) adapter. |
| | show interface InlineGroup | Displays the inline group information. |
| | show interface InlinePort | Displays the inline port information. |
| | show tfo auto-discovery blacklist entries netmask | Displays the auto-discovery blacklist servers table filtered by netmask. |
| | show tfo auto-discovery blacklist statistics | Displays the auto-discovery blacklist server table management statistics. |
| | show tfo synq | Displays the cumulative statistics for the SynQ module. |
| | undebug tfo synq | Disables TFO connection debugging for the SynQ module. |
| Global configuration | adapter epm enable | Enables the EndPoint Mapper (EPM) service. |
| | interface InlineGroup | Sets the InlineGroup of interfaces to configure. |
| | interface InlinePort | Sets an inline port adapter interface to configure. |
| | policy-engine application map basic name WAFS classifier CIFS action optimize full accelerate CIFS-adaptor | Accelerates the traffic using the CIFS accelerator. This new command provides basic policy mapping for WAFS. |
| | tfo auto-discovery blacklist hold-time | Configures a WAE to automatically discover origin servers (such as those servers behind firewalls) that cannot receive TCP packets with setup options and adds these server IP addresses to a blacklist for a specified number of minutes. |
| | tfo auto-discovery blacklist enable | Enables the TFO auto-discovery blacklist operation. |
| | username print-admin-password | Sets the user's print administration password for authentication on a WAAS device. |
| | wccp tcp-promiscuous router-list-num number hash-source-ip | Specifies that the load-balancing hash method should make use of the destination IP address. |
| | wccp tcp-promiscuous router-list-num number hash destination ip | Specifies that the load-balancing hash method should make use of the source IP address. |
| Interface | failover timeout | Sets the maximum time for the inline interface to transition traffic to another port after a failure event. |
| | inline | Enables inline interception for an inlineGroup interface. |

Table 2 lists the commands and options that have changed in WAAS software version 4.0.7.

Table 2 CLI Commands Changed in Version 4.0.7

| Mode | Command and Syntax | Description |
|------|---|---|
| EXEC | show statistics wccp gre | The output of this command now includes the “pass-through packets dropped on assignment update” statistic. This statistic indicates the number of packets that were targeted for TFO pass-through, but were dropped instead because the bucket was not owned by the device. The output of this command has also been changed to include the “packets dropped due to received on loopback” statistic. This statistic indicates the number of packets that were dropped by the WCCP L2 intercept layer because they were received on the loopback interface but were not destined for a local address on the device. |
| EXEC | show wccp gre | The output of this command now includes the “pass-through packets dropped on assignment update” statistic. This statistic indicates the number of packets that were targeted for TFO pass-through, but were dropped instead because the bucket was not owned by the device. The output of this command has also been changed to include the “packets dropped due to received on loopback” statistic. This statistic indicates the number of packets that were dropped by the WCCP L2 intercept layer because they were received on the loopback interface but were not destined for a local address on the device. |
| EXEC | show tfo auto-discovery | The output for this command now includes the SYN retransmission count (for successful connections) and the SYN retransmission resets count fields. |
| EXEC | show statistics tfo pass-through | The output for this command now includes the server blacklist pass-through bytes and packets count fields. |

Table 3 lists the commands and command options that have been removed in WAAS software version 4.0.7.

Table 3 CLI Command Options Removed in Version 4.0.7

| Mode | Command and Syntax | Description |
|----------------------|---|--|
| Global configuration | ip | The dcsp option has been removed. |
| | username | The CIFS-password option has been removed. |
| | wccp tcp-promiscuous | The src-port-mask and dst-port-mask options have been removed. |
| | policy-engine application map adaptor WAFS accept | The policy-engine application map adaptor WAFS accept global configuration command has been removed. |
| | policy-engine application name File-System classifier CIFS-non-wafs action optimize full | The predefined classifier CIFS-non-wafs and its corresponding basic policy mapping with the File-System application has been removed. |

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 4.0.7

To upgrade from WAAS prerelease software to version 4.0.7, 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 4.0.7

When you perform an upgrade to a new WAAS version, first upgrade the WAE devices, and then upgrade the WAE Central Manager devices last.

This section describes the limitations, interoperability considerations, and requirements for upgrading to WAAS 4.0.7 in the following sections:

- [Limitations When Using Mixed Versions in a Network, page 6](#)
- [Version Interoperability Considerations, page 7](#)
- [WAAS Upgrade Requirements, page 8](#)

To take advantage of bug fixes and new features, we recommend that you upgrade your entire deployment to the latest software release.

Limitations When Using Mixed Versions in a Network

If you operate a network with devices that have different software versions, the WAAS Central Manager should be the lowest version. The following limitations exist when you run WAAS 4.0.7 in your network with prior versions of WAAS software:

- The CIFS automatic discovery feature will operate only when both the edge and core WAEs are running software version 4.0.7.
- Inline mode and other new features that appear in the WAAS Central Manager GUI can be configured only by using the CLI if the WAAS Central Manager is running a software version prior to 4.0.7.
- The TFO options propagation feature will operate only when the core WAE is running software version 4.0.7 or later.

Version Interoperability Considerations

When you operate a network with devices that have different software versions, consider the following interoperability issues:

- Software version 4.0.7 does not support the WCCP CIFS caching service (service group 89). If you upgrade the WAAS Central Manager from version 4.0.x to version 4.0.7, and the WCCP CIFS caching service (service group 89) or service masks for the WCCP CIFS caching service were previously configured, these services will be removed during the upgrade.
- WAAS 4.0.7 includes policy-engine map and classifier changes that can cause interoperability issues when you run mixed software versions in your network.

The following policy classifiers were removed in WAAS 4.0.7:

```
classifier CIFS-non-wafs
  match dst port eq 139
  match dst port eq 445
exit
name File-System classifier CIFS-non-wafs action optimize full

map adaptor WAFS accept
  name WAFS all action accelerate cifs
exit
```

The following policy classifier was added in WAAS 4.0.7:

```
classifier CIFS
  match dst port eq 139
  match dst port eq 445
exit
name WAFS classifier CIFS action optimize full accelerate CIFS-adaptor
```

If you attempt to insert a policy using the same classifier as the one used by the **CIFS-adaptor** option, the CLI will fail, and the device will override the device group settings. A warning is logged when this situation occurs.

If you apply the application policy settings from the device group, and any of the policy match conditions of the unsupported policy are being used by the classifier, the device group settings will not override the configuration.

Any modifications to the policy match conditions or classifiers that are being used by the unsupported policies will not be propagated to the CLI.

- When you upgrade the WAE from WAAS 4.0.1 or 4.0.3 to WAAS 4.0.7, the CLI is automatically converted to the new policy format with CIFS acceleration and auto-discovery enabled. If your WAE that is running WAAS 4.0.7 or later is being managed by a Central Manager that is running an earlier version of WAAS, the Central Manager will remove the CIFS classifier match condition that was added in 4.0.7 when it pushes the default policies (from the earlier software version) to the WAE, and both CIFS acceleration and auto-discovery will be disabled.

To work around this issue, use the following procedure to configure the new CIFS policy classifier with ports 139 and 445 from the Central Manager GUI.

- When you upgrade the WAE from WAAS 4.0.5 to WAAS 4.0.7, the CLI is not automatically converted to the new policy format, and the CIFS acceleration and auto-discovery features do not work. To work around this issue, use the following procedure to add the new CIFS classifier with ports 139 and 445 from the Central Manager GUI.

To add the configuration to multiple devices simultaneously, configure the new classifier for a device group. To add the new CIFS 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 policy that you want to edit.
 - Step 3** Click the **New Classifier** icon and create a new classifier named **CIFS** with the following two match conditions:
 - Destination Port Start: **139**
 - Destination Port Start: **445**
 - Step 4** To save the configuration, click **Submit**.
-

Using the CLI, configure each of your devices as follows:

```
WAE(config)# policy-engine application map basic name WAFS classifier CIFS action
optimize full accelerate CIFS-adaptor
```

- After you upgrade from any 4.0.x version to version 4.0.7, the CIFS-non-wafs classifier configuration remains. You must delete the CIFS-non-wafs classifier and its policy map after the upgrade.
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 from WAAS version 4.0.x to 4.0.7, one of the CIFS classifier match conditions is removed again. To workaround this issue, use the Central Manager GUI to edit the CIFS classifier and add a match condition with Destination Port Start: 445.

WAAS Upgrade Requirements

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 9](#).) 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 WAFS 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 [“WAAS Upgrade Requirements” section on page 8.](#))

Operating Considerations

This section includes operating considerations that apply to software version 4.0.7:

- [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](#)
- [Configuring a WAE for Maximum Performance on High Bandwidth Delay Product \(BDP\) Links](#)
- [Disabling the Automatic Machine Account Password Changes for the Edge WAE](#)
- [Using PortFast with Inline Mode](#)
- [Cabling the Cisco WAE Inline Network Adapter](#)

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.

Configuring a WAE for Maximum Performance on High Bandwidth Delay Product (BDP) Links

Cisco WAAS can be deployed in different network environments, involving multiple link characteristics (bandwidth, latency, packet loss, etc.). All systems are optimized by default to accommodate networks with maximum Bandwidth Delay Product (BDP) up to the values listed below:

- WAE-511/512: DefaultBDP = 32KB
- WAE-611/612: DefaultBDP = 512KB
- WAE-7326: DefaultBDP = 2048KB

In cases where higher bandwidth is available or higher latencies are involved, replace BDP with 2048KB. Use the following example to configure BDP from the WAAS CLI:

```
#config t
(config)#tfo tcp optimized-receive-buffer BDP
(config)#tfo tcp optimized-send-buffer BDP
(config)#exit
#write
```

To configure BDP from the WAAS Central Manager GUI, follow these steps:

-
- Step 1** Go to **Devices > Devices** or **Device Groups**.
 - Step 2** Click the **Edit** icon next to the device for which you want to configure BDP.
 - Step 3** From the Contents pane, select **Acceleration >Acceleration TCP Settings**.

- Step 4** In the Receive Buffer Size > Optimized Side field, apply the BDP value as calculated above.
 - Step 5** In the Send Buffer Size > Optimized Side field, apply the BDP value as calculated above.
 - Step 6** Click **Submit**. Changes will be applied within a configuration distribution cycle (default 5 min).
-

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.

Cabling the Cisco WAE Inline Network Adapter

The inline network adapter ships with two types of cables: crossover and straight-through. When you connect the WAE inline network adapter, proper cabling depends on the link speed (Gigabit Ethernet or Fast Ethernet) and the types of devices (DCE or DTE) being connected.



Note

You must retain the same link speed from one end of the connection to the other end. Inline adapter interfaces are able to autonegotiate link speeds. If any of your connecting interfaces are configured for Fast Ethernet (whether on a switch or a router), your WAE inline adapter uses Fast Ethernet. If any of your connecting interfaces are configured for Gigabit Ethernet, your WAE inline adapter uses Gigabit Ethernet. Speed and duplex settings are port specific, so two inline ports can negotiate different speeds independently.

If you are connecting a WAE inline appliance between two devices using Gigabit Ethernet, you can use either straight-through cables, crossover cables, or any combination of the two cable types, regardless of the type of device. However, for consistency, we recommend that you use straight-through cables for all Gigabit Ethernet connections.

Table 4 shows the cable requirements for WAE and non-WAE connections when you are using Gigabit Ethernet end to end.

Table 4 Cable Requirements for WAE Connections Using Gigabit Ethernet

| Connection | Required Cable |
|------------------------------------|-------------------------------|
| Switch to switch (no WAE) | Crossover or Straight-through |
| Switch to router (no WAE) | Crossover or Straight-through |
| Router to router (no WAE) | Crossover or Straight-through |
| Switch to WAE and WAE to Router | Crossover or Straight-through |
| Switch to WAE and WAE to Switch | Crossover or Straight-through |
| Router to WAE and WAE to Router | Crossover or Straight-through |
| WAE to WAE | Crossover or Straight-through |

If you are connecting to Fast Ethernet ports on both the LAN and the WAN sides of the WAE inline appliance, you must consider the types of devices that are being connected, and you must use the correct cables.

Table 5 shows the cable requirements for WAE and non-WAE connections when you are using Fast Ethernet end to end. (For complete cabling instructions, see *Installing the Cisco WAE Inline Network Adapter*.)

Table 5 Cable Requirements for WAE Connections Using Fast Ethernet

| Connection | Required Cable |
|------------------------------------|--------------------------------------|
| Switch to switch (no WAE) | Crossover |
| Switch to router (no WAE) | Straight-through |
| Router to router (no WAE) | Crossover |
| Switch to WAE and WAE to Router | Straight-through Crossover |
| Switch to WAE and WAE to Switch | Straight-through Straight-through |
| Router to WAE and WAE to Router | Straight-through Straight-through |
| WAE to WAE | Crossover |

Documentation Correction

The following statement applies to the WAAS 4.0.7 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 4.0.7 Open and Resolved Caveats

The following sections list the open and resolved caveats for software version 4.0.7:

- [Software Version 4.0.7 Open Caveats](#)
- [Software Version 4.0.7 Resolved Caveats](#)

Software Version 4.0.7 Open Caveats

The following caveats apply to software version 4.0.7:

- **CSCse71473**—After changing a local user’s password, where 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) breaks connections if it does not intercept both traffic directions, so EPM-based applications are unavailable in asymmetric routing scenarios. This situation occurs when a WAE has visibility to only one side of a TCP connection. Because of router configuration or network topology, the return traffic bypasses the WAE. For example, this would occur if WCCP redirection is configured on some router interfaces but not all. When using WCCP redirection in, a router with two WAN and one LAN interface must have interception configured on all three WAN and LAN interfaces. If one WAN interface is omitted, EPM traffic from that interface

will not be handled properly. Workaround: Ensure that both WCCP service groups 61 and 62 are on the same interface, which is the WAN interface that connects to another WAE-accelerated site. Alternatively, configure WCCP redirection in on all relevant interfaces.

- **CSCsg24304**—Flow protection may stop working and active connections may hang or be reset when new WAEs are added to the WCCP cache farm. This problem is seen when an FTP Get request is made to request a large file from a server in the data center and the request is served through one of the WAEs in the WCCP cache farm. At the same time, a new WAE is added to the existing WCCP cache farm and causes the recalculated hash/mask assignment to redirect the FTP request to the new WAE. Workaround: Add or remove WAEs from the WCCP cache farm only when the traffic through the WAEs is light or nonexistent.
- **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 retransmission in the Windows clients 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:
 1. Ensure the WAAS Central Manager has the correct time.
 2. Execute the following CLI commands on the WAAS Central Manager:


```
CentralManager# configure
CentralManager(config)# central-manager role primary
CentralManager(config)# cms enable
```
 3. 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.
- **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 4.0.7 Resolved Caveats

The following caveats were resolved in software version 4.0.7:

- **CSCse61335**—Starting in calendar year 2007, daylight saving summer-time rules may cause WAAS to generate time stamps (such as in syslog messages) that are off by one hour.
- **CSCse62556**—When trying to access the ~snapshot folder on a Netapp file server using the “.snapshot” name, the folder is inaccessible using WAFS.
- **CSCse64582**—CIFS (WAFS) disconnected read mode does not work after reloading an edge WAE. The client receives an ‘Internal Error’ message and the filer is not available in disconnected mode.
- **CSCse99631**—When you restore the database on a CM, CLI commands that you configured through the GUI retain their default settings.
- **CSCsf18895**—The **ip default-gateway** command does not get applied in the WAE.
- **CSCsg14550**—WCCP service 89 does not perform a WCCP bypass return for CIFS servers that are not in the WAFS accept list. WCCP service 89 was removed.
- **CSCsg29584**—File corruption issues occur when shared Excel files are being concurrently modified by several users.
- **CSCsg39746**—During the logon script, the user is not allowed to map to a network drive through the DFS root. Mapping to the same server directly (not through DFS) works correctly.

- **CSCsg44521**—When WCCP GRE is configured, if the WCCP router fragments a packet, and the first packet fragment does not contain all of the original packet’s IP header information, the WAE will drop the packet.
- **CSCsg50460**—The CMS status becomes offline and restarts when you select a printer driver to be downloaded and then deselect the driver while it is being downloaded by device.
- **CSCsg55742**—Multiple security vulnerabilities as documented in the Cisco Security Response “Multiple vulnerabilities in OpenSSL library” at <http://www.cisco.com/warp/public/707/cisco-sr-20061108-openssl.shtml>.
- **CSCsg60239**—The CMS import fails during an upgrade from WAFS to WAAS. Workaround: Manually apply changes where needed and then restart the management service.
- **CSCsg66994**—A core file is created when the WAE queries the hrStorageTable MIB.
- **CSCsg75506**—The error message severity for RPC requests to the EPM with “opnums=3” needs to be changed from 4 (warning) to 7 (debug).
- **CSCsg78235**—Directories are being deleted, and a number of processes are running repeatedly, causing resource issues and poor performance.
- **CSCsg79612**—During an attempt to run a preposition task, the file server issues an “access denied” error message.
- **CSCsh04752**—When the link on one interface goes down, the link state needs to be communicated to the other interfaces so that the router and switch will stop routing through that link.
- **CSCsh16100**—A large RSYNC transfer appears to hang or not finish.
- **CSCsh21715**—CIFS acceleration does not work if the CM is configured to export more than 1000 file servers.
- **CSCsh39574**—The Flash image is corrupted when you use the **restore factory-default preserve basic-config** command.
- **CSCsh41681**—Packets are generated using an invalid tuple after tcp-proxy releases resources.
- **CSCsh48911**—The execute from remote mode fails with the following error message: “File is used by another application.”
- **CSCsh53369**—WCCP statistics for non-GRE/non-WCCP statistics is increasing for no apparent reason.
- **CSCsh53377**—CMS is stopping/starting WCCP and resetting WCCP configuration periodically.
- **CSCsh53396**—WCCP reassignments (RA) cause high CPU usage on the Catalyst 6500 series switch.
- **CSCsh53668**—Slow file transfers occur from Citrix ICA server to local client when the files go through the WAE.
- **CSCsh54130**—SQL queries do not work when you use an SQL server that is using the NetBIOS protocol (port 139).
- **CSCsh55119**—The Central Manager displays the following alerts: device crash / core files or core file found in /local1/core_dir on a device.
- **CSCsh56736**—A core dump in tcp-proxy occurs.
- **CSCsh65404**—A core dump in tcp-proxy occurs because a message is too large for DRE to cache.
- **CSCsh69586**—When disabling the EPM on a remote side, the CM sees major alarms that relate to the keepalives for the EPM.
- **CSCsh70666**—The WAAS TFO transaction log export operation fails.

- **CSCsh71218**—TFO connections linger long after the TCP connections are closed.
- **CSCsh71886**—The WAE-7326 hangs with no ping, telnet, or console access.
- **CSCsh72261**—A WAE that runs WCCP with a single connection between the client and server, enters KDB mode.
- **CSCsh75192**—A remote Windows installation fails.
- **CSCsh78511**—The SNMP agent crashes when any of the MIB objects that are found in the hrStorageTable or hrFStable MIB are queried repeatedly.
- **CSCsh83507**—Clients that are operating with servers that support NTFS data streams receive an error during the copy, delete, or rename operations, and nonexistent files, such as “filename:\$\$DATA” may be seen in the directory listing.

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, CCSI, CCENT, Cisco Eos, Cisco HealthPresence, the Cisco logo, Cisco Lumin, Cisco Nexus, Cisco Nurse Connect, Cisco Stackpower, Cisco StadiumVision, Cisco TelePresence, Cisco WebEx, DCE, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn and Cisco Store 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. (0903R)

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.

