Troubleshooting Your WAAS Network

This chapter describes the troubleshooting and diagnostics tools available in the Cisco WAAS Central Manager that can help you identify and resolve issues with your WAAS system.

For additional advanced Cisco WAAS troubleshooting information, see the *Cisco WAAS Troubleshooting Guide for Release 4.1.3 and Later* on Cisco DocWiki. For information on flow monitoring, see Configuring Flow Monitoring in Chapter 15, "Monitoring Your WAAS Network."

Note Throughout this chapter, the term Cisco WAAS device is used to refer collectively to the WAAS Central Manager and Cisco Wide Area Application Engines (WAEs) in your network. The term WAE refers to WAE and Wide Area Application Virtual Engine (WAVE) appliances, Cisco Service Ready Engine Service Module (SRE-SM) modules running WAAS, and Cisco Virtual WAAS (vWAAS) instances.

This chapter contains the following sections:

- WAAS Troubleshooting Guidelines
- Gathering WAAS Troubleshooting Information
- Verifying the WAAS Image
- WAAS Central Manager Alarm Panel
- Troubleshooting Devices Using Alerts
- Using the show and clear Commands from the Central Manager
- Configuring and Viewing Logs
- Using Diagnostic Tests
- Using the Kernel Debugger
- Using WAAS TCP Traceroute
- Verifying WAAS Physical Connectivity
- Contacting Cisco Technical Support

WAAS Troubleshooting Guidelines

To troubleshoot your WAAS system, follow these general guidelines:

Table 16-1 Troubleshooting Guidelines

Troubleshooting Guideline	Description
1. Maintain a consistent and recommended software version across all your WAAS devices.	• If versions must differ, the Central Manager must be running the highest version. See Verifying the Current WAAS Image to determine the version in use.
2. See the WAAS Release Note for your software version.	• See the *Release Note for Cisco Wide Area Application Services* for the latest features, operating considerations, caveats, and CLI command changes.
3. Before you introduce configuration changes on the WAAS Central Manager, use the CMS backup feature to save your configuration.	• If you run into problems with the new configuration, you can restore the previous configuration. See the “Backing Up and Restoring your WAAS System” section in he *Cisco Wide Area Application Services Configuration Guide* for tthe Cisco Wide Area Application Services Configuration Guide. Troubleshoot any problems with new configuration changes immediately after making them.
4. Verify that your configuration is correct for your network application.	• Make any required changes to the running-config file, and then test the configuration. If it is satisfactory, save it to the startup-config file using the copy running-config startup-config command.
5. Enable system message logging.	• See Configuring and Viewing Logs.
6. Run the diagnostic tool to verify device functionality and connectivity.	• See Using Diagnostic Tests.
7. Verify the physical connectivity between WAAS peers and to the application servers.	• See Verifying WAAS Physical Connectivity.
8. Gather information that defines the specific symptoms.	• See Gathering WAAS Troubleshooting Information.
9. Troubleshooting other problems:	• For further information on problems including hardware or disk problems, or the system passing through more traffic than it is optimizing, see the *Cisco WAAS Troubleshooting Guide for Release 4.1.3 and Later*.
10. After you have determined that your troubleshooting attempts have not resolved the problem, contact the Cisco Technical Assistance Center (TAC) or your technical support representative.	• See Contacting Cisco Technical Support.

Gathering WAAS Troubleshooting Information

This section contains the following topics:

- Rebooting the WAAS Device
- Using the copy tech-support Command
- Using show Commands
- Using show Commands for WCCP Deployments
- Generating a System Report
- Capturing and Analyzing Packets

Rebooting the WAAS Device

Caution Do not reboot the WAAS device unless it is absolutely necessary. Some information that is important to troubleshooting may not survive a reboot. Try to gather as much information as possible before rebooting.

Using the copy tech-support Command

In most cases, you can gather the information you need to troubleshoot the device with the **copy tech-support** command. This command runs many **show** commands that are useful for troubleshooting, and it gathers the output into a single file.

You can redirect the output of the **copy tech-support** command to a disk file, an FTP server, or a TFTP server, using the following syntax:

copy tech-support {**disk** *filename* | **ftp** {*hostname* | *ip-address*} *remotedirectory remotefilename* | **tftp** {*hostname* | *ip-address*} *remotefilename*}

Using show Commands

You can use several **show** EXEC commands to gather information specific to the symptoms you are observing in your device.

- **show alarms**
- **show accelerator**
- **show license**
- **show statistics connection**
- **show statistics tfo**
- **show interface**

Using show Commands for WCCP Deployments

For WCCP deployments, use the following commands on the WAE:

- **show wccp gre**
- **show wccp routers**
- **show wccp wide-area-engine**
- **show wccp flows**
- **show egress-methods**

For WCCP deployments, use the following commands on the router or switch (for each service group, where applicable):

- **show ip wccp**
- **show ip wccp interfaces detail**
- **show ip wccp** *service*

- **show ip wccp** *service* **detail**

For WCCP deployments when hashing is used, use the following commands on the router or switch:

- **show tcam counts**
- **show mls stat**
- **show mls netflow table detail**
- **show mls netflow ip count**
- **show mls netflow ip sw-installed count**
- **show mls netflow ip sw-installed detail**
- **show fm inteface** *interface_name*

For WCCP deployments when masking used, use the following commands on the router or switch:

- **show ip wccp** *service* **mask**
- **show ip wccp** *service* **merge**
- **show tcam interface** *interface_name acl* {**in** | **out**} **ip**
- **show tcam interface** *interface_name acl* {**in** | **out**} **ip detail**

Generating a System Report

A system report (sysreport) is a comprehensive report that you will need before you contact Cisco technical support. You can generate a sysreport by running the **copy sysreport** command.

The system report contains the output from many commands and logs on the system, including **show** commands, network statistics, graphs, log contents, configuration settings and statistics. It can take some time to generate a system report and it can be from 30 - 100 MB in size or larger. The system report contains many more elements than are included in the **copy tech-support** command, and is generally needed when contacting Cisco technical support.

Consider these guidelines when you generate a system report:

- Before generating a system report, use the **test** command to run the diagnostic tests so that this information is included in the system report.
- When generating a system report on a Central Manager (or standby Central Manager), you should first make a database backup by using the cms database backup command.
- When generating a system report, do not use any command options that limit the report to a specific time period, as this could cause information even within that time period not to be included.

To generate a sysreport and store it to an FTP server, use this form of the command:

copy sysreport ftp *server-ip remote-directory remote-file-name*

For example:

```
wae# copy sysreport ftp 10.10.10.5 /reports wae1report
```

Capturing and Analyzing Packets

Capturing packets (sometimes referred to as a "TCP dump") is a useful aid in troubleshooting connectivity problems with the WAAS device or for monitoring suspicious activity.

The WAAS device can track packet information for network traffic that passes through it. The attributes of the packet are defined by an ACL. The WAAS device buffers the captured packets, and you can copy the buffered contents to a file or to a remote server. You can also display the captured packet information on your console or terminal.

Two packet capture utilities are available: **tcpdump** and **tethereal**. These commands require admin privileges.

Consider these guidelines when you use **tcpdump** or **tethereal** to capture packets:

- By default, these commands capture only the first 64 bytes of each packet. We recommend that you use the **-s 1600** option to capture full packet data.
- If you will be taking large traces, use **tcpdump** to create rolling packet captures in multiple files. (The **-C** option sets the maximum size of each captured file in KB and the **-M** option sets the maximum number of log files to create.)
- If you need to filter the packets captured, use **tethereal** with the **-R read** filter option. You can use tcpdump to create a large packet capture, then use tethereal against the captured file to perform filtering.
- Be careful when using tcpdump in a WCCP environment because tcpdump filters do not look within the GRE wrapper. You will need to use tethereal if you need to do that.
- With both commands, use the **-i any** option to capture all interfaces, or separate telnet sessions to capture on separate interfaces. Use **^c** (CTRL+c) to stop the packet capture.
- For detailed information on how to use **tcpdump** and **tethereal**, see the *Cisco Wide Area Application Services Command Reference*.

There are several packet analysis tools that you can use to analyze packet capture files after you have captured them, including Wireshark, Ethereal, Microsoft Netmon and Sniffer Pro.

Verifying the WAAS Image

This section contains the following topics:

- Verifying the Current WAAS Image
- Verifying a Pending WAAS Image

Verifying the Current WAAS Image

Use the **show version** command to display the version of the software image that is currently running in your WAAS device. The command output includes:

- Copyright information
- Software Release number, for example:
  “Cisco Wide Area Application Services Software Release 6.2.3
- Device model and WAAS Version, for example:
  oe-vwaas-6.2.3.17
- Most recent compiled date and time
- Most recent restart date and time
- Device uptime, weeks, hours, minutes, and seconds

You can use the show version command from the CLI or from the WAAS Central Manager:

*To use the **show version** command from the CLI:*

```
wae# show version
```

*To use the **show version** command from the WAAS Central Manager:*

Step 1 Navigate to **Devices** > *DeviceName* > **Monitor** > **CLI Commands** > **show commands**

Step 2 From the show commands dropdown list, select **show version**

Step 3 Click **Submit**.

Verifying a Pending WAAS Image

Use the **show version pending** to verify that there is no pending software upgrade (waiting for a device reboot). You should see the message "No pending version".

You can use the show version command from the CLI or from the WAAS Central Manager:

*To use the **show version pending** command from the CLI:*

```
wae# show version pending
```

*To use the **show version pending** command from the WAAS Central Manager:*

Step 1 Navigate to **Devices** > *DeviceName* > **Monitor** > **CLI Commands** > **show commands**

Step 2 From the show commands dropdown list, select **show version**

Step 3 In the Arguments field, enter **pending**.

Step 4 Click **Submit**.

WAAS Central Manager Alarm Panel

This section has the following sections:

- Viewing the Alarm Panel
- Acknowledging an Alarm
- Filtering and Sorting Alarms
- Device Alarms

Viewing the Alarm Panel

The alarm panel provides a near real-time view of incoming alarms and refreshes every two minutes to reflect updates to the system alarm database.

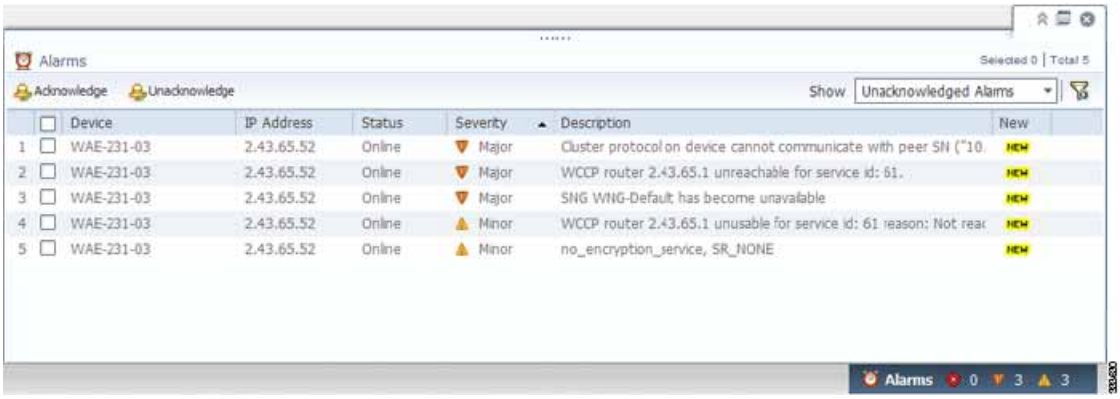
To view the alarms panel, click **Alarms** at the bottom right side of the Central Manager window.

Only Active alarms can be acknowledged in the alarm panel. Pending, Offline, and Inactive alarms cannot be acknowledged in the alarm panel.

The alarm panel also allows you to filter your view of the alarms in the list. Filtering allows you to find alarms in the list that match the criteria that you set.

Figure 16-1 shows the alarm panel.

Figure 16-1 Alarm Panel



Acknowledging an Alarm

To acknowledge an active alarm, follow these steps:

Step 1 In the alarm panel, check the check box next to the name of the alarm that you want to acknowledge.

Step 2 Click the **Acknowledge** taskbar icon.

The **Acknowledge Alarm Comments** dialog box that allows you to enter comments about the alarm is displayed.

Step 3 Enter a comment and click **OK**. Alternatively, click **Cancel** to return to the alarm panel without completing the acknowledge action.

Comments enable you to share information about the cause or solution of a particular problem that caused the alarm. The comments field accepts up to 512 characters. You can use any combination of alpha, numeric, and special characters in this field.

Filtering and Sorting Alarms

To filter and sort the alarms displayed in the alarm panel, follow these steps:

Step 1 From the Show drop-down list, choose one of the following filtering options:

- **All**
- **Quick Filter**
- **Unacknowledged Alarms**
- **Acknowledged Alarms**

- **Alarms for** *device-name* (shown in the device context)

Step 2 If you chose Quick Filter, enter the match criteria in one or more fields above the list.

Step 3 To sort alarm entries, click a column header.

Entries are sorted alphabetically (in ASCII order). The sort order (ascending or descending) is indicated by an arrow in the column header.

Step 4 Choose **All** to clear the filter.

Device Alarms

Device alarms are associated with device objects and pertain to applications and services running on your WAAS devices. Device alarms are defined by the reporting application or service. Device alarms can also reflect reporting problems between the device and the WAAS Central Manager GUI. Table 16-2 describes the various device alarms that can appear.

Table 16-2 Device Alarms for Reporting Problems

Alarm	Alarm Severity	Device Status	Description
Device is offline	Critical	Offline	The device has failed to communicate with the WAAS Central Manager.
Device is pending	Major	Pending	The device status cannot be determined. This status can appear after a new device is registered, but before the first configuration synchronization has been performed.
Device is inactive	Minor	Inactive	The device has not yet been activated or accepted by the WAAS Central Manager.
Device has lower software version	Minor	Online	The device has an earlier software version than the WAAS Central Manager, and it may not support some features.

Troubleshooting Devices Using Alerts

The WAAS Central Manager GUI allows you to view the alarms on each device and troubleshoot a device in the Troubleshooting Devices window.

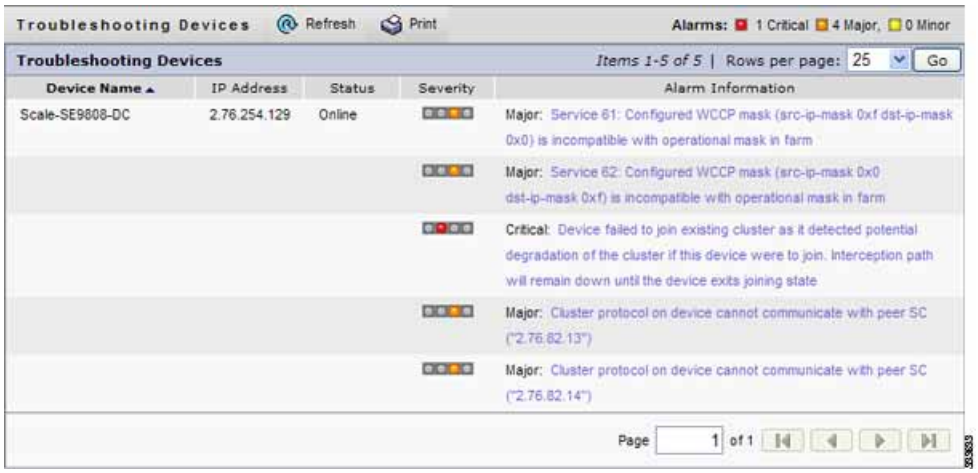
To troubleshoot a device from the Troubleshooting Devices window, follow these steps:

Step 1 From the WAAS Central Manager menu, choose **Devices > All Devices**.

Step 2 Click the device alarm light bar in the Device Status column to view the alarms on a single device.

The Troubleshooting Devices pane appears, either in the WAAS Central Manager window or as a separate dialog box. (See Figure 16-2.)

Figure 16-2 Troubleshooting Devices Window



Step 3 In the Alarm Information column, hover your mouse over an alarm message until the Troubleshooting tools contextual menu appears. The pop-up menu provides links to the troubleshooting and monitoring windows in the WAAS Central Manager GUI.

Step 4 From the drop-down list that is displayed, choose the troubleshooting tool that you want to use, and click the link. The link takes you to the appropriate window in the WAAS Central Manager GUI. Table 16-3 describes the tools available for device alarms.

You can view the Troubleshooting Devices window for all devices by choosing **Monitor** > **Troubleshoot** > **Alerts** from the global context.

Table 16-3 Troubleshooting Tools for Device Alarms

Item	Navigation	Description
Update Software	Choose *device*, **Admin** > **Versioning** > **Software Update**	Displays the Software Update window for this device. Appears only if the device software version is lower than that of the Central Manager.
Edit/Monitor Device	Device dashboard	Displays the Device Dashboard for configuration.
Telnet to Device	Opens a Telnet window	Initiates a Telnet session using the device IP address.
View Device Log	Choose *device*, **Admin** > **History** > **Logs**	Displays system message logs filtered for this device.
Run Show Commands	Choose *device*, **Monitor** > **CLI Commands** > **show Commands**	Displays the device **show** command tool. For more information, see Using the show and clear Commands from the Central Manager.

Using the show and clear Commands from the Central Manager

You can use the **show** and **clear** EXEC commands from either the WAAS CLI or the WAAS Central Manager. To use the **show** and **clear** command from the CLI, see the *Cisco Wide Area Application Services Command Reference*.

To use the **show** and **clear** commands from the WAAS Central Manager, follow these steps:

Step 1 From the WAAS Central Manager menu, choose **Devices** > *device-name*.

Step 2 Choose **Monitor** > **CLI Commands** > **Show Commands** or **Clear Commands**.

Step 3 From the Command drop-down list, choose either a **show** or **clear** command.

Step 4 Enter arguments for the command, if any.

Step 5 Click **Submit** to display the command output.

A window displays the command output for that device.

Note The **show** and **clear** CLI commands that are available differ depending on the type of device that you select.

Configuring and Viewing Logs

This section contains the following topics:

- Configuring System Logging
- Configuring Transaction Logging
- Viewing the System Message Log
- Viewing the Audit Trail Log
- Viewing a Device Log
- CLI Commands for Verifying and Viewing Logs and System Image

Configuring System Logging

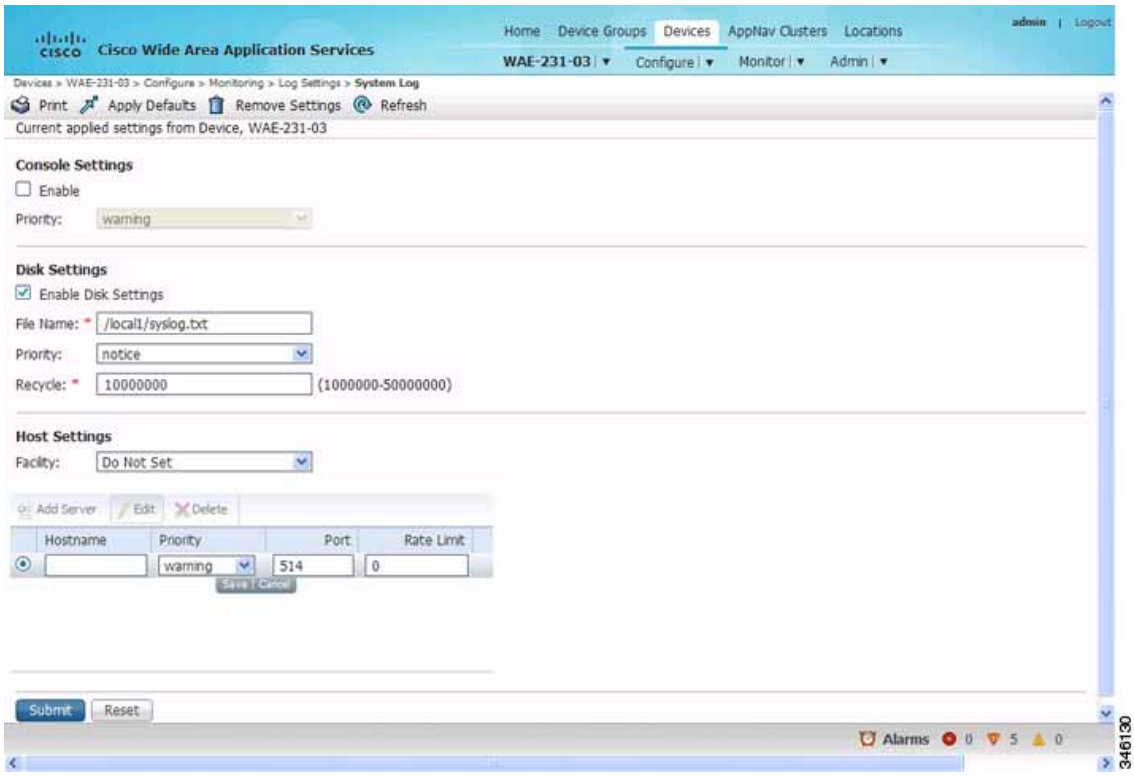
Use the WAAS system logging feature to set specific parameters for the system log file (syslog). This file contains authentication entries, privilege-level settings, and administrative details. The system log file is located in the system file system (sysfs) partition as /local1/syslog.txt.

To enable system logging, follow these steps:

Step 1 From the WAAS Central Manager menu, choose **Devices** > *device-name* **(**or **Device Groups** > *device-group-name*).

Step 2 Choose **Configure** > **Monitoring** > **Log Settings** > **System Log**. The System Log Settings window appears. (See Figure 16-3.)

Figure 16-3 System Log Settings Window



Step 3 Enable system log files to be sent to the console:

a. In the Console Settings section, check the **Enable** check box.

b. From the Priority drop-down list, choose the severity level of the message that should be sent to the specified remote syslog host. The default priority-code is *warning* (level 4). Each syslog host is capable of receiving a different level of event messages. (See Table 16-4 for a list of priority levels.)

Step 4 Enable syslog files to be sent to a disk:

a. In the Disk Settings section, check the **Enable Disk Settings** check box. This setting is checked by default.

b. In the File Name field, enter a path and a filename where the syslog files will be stored on a disk.

c. From the Priority drop-down list, choose the severity level of the message that should be sent to the specified remote syslog host. The default priority code is *warning* (level 4). Each syslog host is capable of receiving a different level of event messages. (See Table 16-4 for a list of priority levels.)

d. In the Recycle field, specify the size of the syslog file (in bytes) that can be recycled when it is stored on a disk. (The default value of the file size is 10000000.)

Whenever the current log file size surpasses the recycle size, the log file is rotated. (The default recycle size for the log file is 10,000,000 bytes.) The log file cycles through a maximum of five rotations, and each rotation is saved as *log_file_name.[1-5]* under the same directory as the original log.

The rotated log file is specified in the File Name field (or by using the **logging disk filename** command).

Step 5 Enable syslog files to be sent to a host server:

a. In the Host Settings section, from the Facility drop-down list, choose the appropriate facility.

b. Click the **Add Server** taskbar icon above the host server list. You can add up to four host servers to which syslog messages can be sent. For more information.

c. In the Hostname field, enter a hostname or IP address (IPv4 or IPv6) of the remote syslog host. You must specify at least one hostname if you have enabled system logging to a host.

d. From the Priority drop-down list, choose the severity level of the message that should be sent to the specified remote syslog host. The default priority code is *warning* (level 4). Each syslog host is capable of receiving a different level of event messages. (See Table 16-4 for a list of priority levels.)

e. In the Port field, specify the destination port on the remote host to which the WAAS device should send the message. The default port number is 514.

f. In the Range Limit field, specify the number of messages per second that are allowed to be sent to the remote syslog host. To limit bandwidth and other resource consumption, messages to the remote syslog host can be rate limited. If this limit is exceeded, the specified remote syslog host drops the messages. There is no default rate limit, and by default, all syslog messages are sent to all of the configured syslog hosts.

Step 6 Click **Submit**.

To configure system logging from the CLI, you can use the **logging** global configuration command.

This section contains the following topics:

- Priority Levels
- Multiple Hosts for System Logging

Priority Levels

Table 16-4 lists the different priority levels of detail that can be sent to the recipient of syslog messages for a corresponding event.

Table 16-4 System Logging Priority Levels and Descriptions

Priority Code	Condition	Description
0	Emergency	System is unusable.
1	Alert	Immediate action needed.
2	Critical	Critical conditions.
3	Error	Error conditions.
4	Warning	Warning conditions.
5	Notice	Normal but significant conditions.
6	Information	Informational messages.
7	Debug	Debugging messages.

Each syslog host can receive different priority levels of syslog messages. You can configure different syslog hosts with a different syslog message priority code to enable the WAAS device to send varying levels of syslog messages to the four external syslog hosts. For example, a WAAS device can be configured to send messages that have a priority code of *error* (level 3) to the remote syslog host that has an IP address of 10.10.10.1 and messages that have a priority code of *warning* (level 4) to the remote syslog host that has an IP address of 10.10.10.2.

Note Setting a logging priority to Levels 1-4 can be CPU-intensive, and can generate a large amount of output.

To achieve syslog host redundancy or failover to a different syslog host, you must configure multiple syslog hosts on the WAAS device and assign the same priority code to each configured syslog host, for example, assigning a priority code of *critical* (level 2) to syslog host 1, syslog host 2, and syslog host 3.

In addition to configuring up to four logging hosts, you can also configure the following for multiple syslog hosts:

- A port number that is different from the default port number, 514, on the WAAS device to send syslog messages to a logging host.
- A rate limit for the syslog messages, which limits the rate at which messages are sent to the remote syslog server (messages per second) in order to control the amount of bandwidth used by syslog messages.

Multiple Hosts for System Logging

Each syslog host can receive different priority levels of syslog messages. You can configure different syslog hosts with a different syslog message priority code to enable the WAAS device to send varying levels of syslog messages to the four external syslog hosts. For example, a WAAS device can be configured to send messages that have a priority code of *error* (level 3) to the remote syslog host that has an IP address of 10.10.10.1 and messages that have a priority code of *warning* (level 4) to the remote syslog host that has an IP address of 10.10.10.2.

To achieve syslog host redundancy or failover to a different syslog host, you must configure multiple syslog hosts on the WAAS device and assign the same priority code to each configured syslog host, for example, assigning a priority code of *critical* (level 2) to syslog host 1, syslog host 2, and syslog host 3.

In addition to configuring up to four logging hosts, you can also configure the following for multiple syslog hosts:

- A port number that is different from the default port number, 514, on the WAAS device to send syslog messages to a logging host.
- A rate limit for the syslog messages, which limits the rate at which messages are sent to the remote syslog server (messages per second) in order to control the amount of bandwidth used by syslog messages.

Configuring Transaction Logging

This section contains the following topics:

- Enabling Transaction Logging
- Transaction Logs

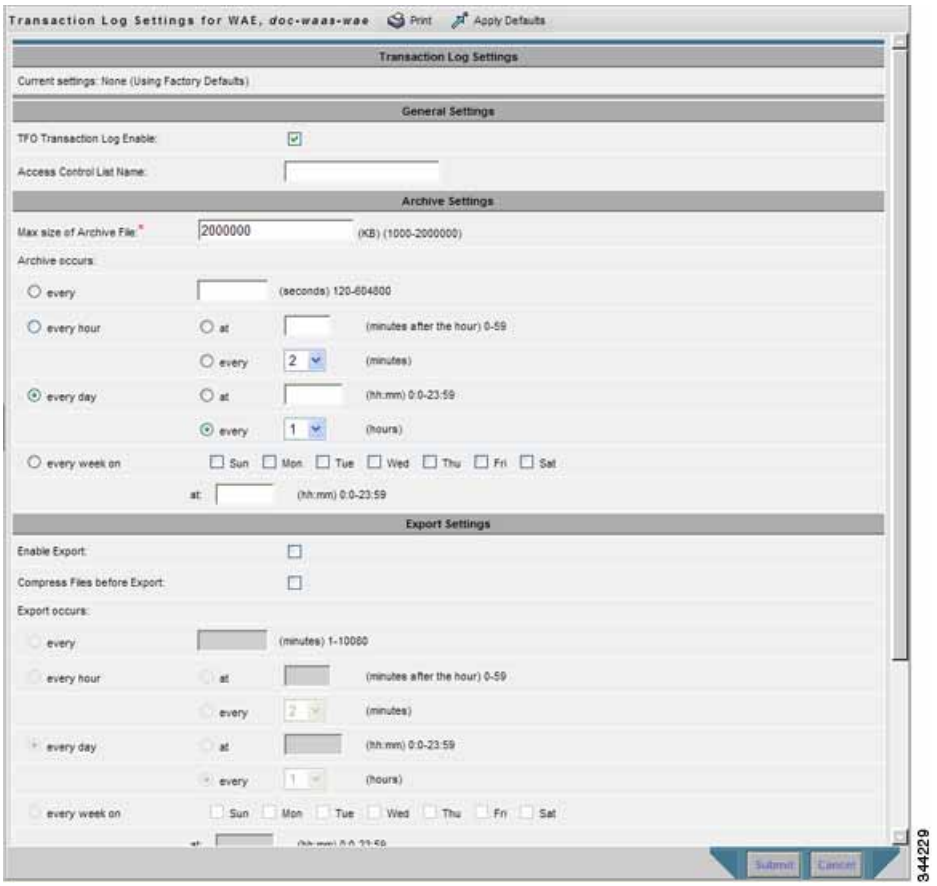
Enabling Transaction Logging

To enable transaction logging for TFO flows and video streams, follow these steps:

Step 1 From the WAAS Central Manager menu, choose **Devices** > *device-name* (or **Device Groups** > *device-group-name*).

Step 2 Choose **Configure** > **Monitoring** > **Log Settings** > **Transaction Log** for TFO transaction logging or **Configure** > **Monitoring** > **Log Settings** > **Video Acceleration Transaction Log** for video transaction logging. The Transaction Log Settings window appears. (See Figure 16-4.) (The Video Transaction Log Settings window looks the same, but does not include the General Settings area at the top.)

Figure 16-4 Transaction Log Settings Window



Step 3 Under the General Settings area title, check the **TFO Transaction Log Enable** check box to enable transaction logging. (This check box does not appear for video transaction logging.)

The fields on the window become active.

Step 4 (Optional) In the Access Control List Name field, enter the name of an access control list that you want to use to limit transaction logging. If you specify an access control list, only transactions from hosts that are defined in that access list are logged. (This field does not appear for video transaction logging.)

Use the **ip access-list** global configuration command to define an access list.

Step 5 Under the Archive Settings area title, specify values for the following fields:

- Max Size of Archive File—Maximum size (in kilobytes) of the archive file to be maintained on the local disk. This value is the maximum size of the archive file to be maintained on the local disk. The range is 1000 to 2000000. The default is 2000000.
- Archive Occurs Every (interval)—Interval at which the working log data is cleared and moved into the archive log.

Step 6 Configure the fields in the Export Settings area to export the transaction log file to an FTP server.

Table 16-5 describes the fields in the Export Settings area.

Table 16-5 Export Settings

Field	Function
Enable Export	Enables transaction logging to be exported to an FTP server.
Compress Files before Export	Enables compression of archived log files into gzip format before exporting them to external FTP servers.
Export occurs every (interval)	Interval at which the working log should be cleared by moving data to the FTP server.
Export Server	The FTP export feature can support up to four servers. Each server must be configured with a username, password, and directory that are valid for that server. • Export Server—The IP address or hostname of the FTP server. • Name—The user ID of the account used to access the FTP server. • Password/Confirm Password—The password of the FTP user account specified in the Name field. You must enter this password in both the Password and Confirm Password fields. Do not use the following characters: space, backward single quote (`), double quote ("), pipe (|), or question mark (?). • Directory—The name of a working directory that will contain the transaction logs on the FTP server. The user specified in the Name field must have write permission to this directory. • SFTP—If the specified FTP server is a secure FTP server, check the **SFTP** check box.

Step 7 Click **Submit**.

A **`Click Submit to Save`** message appears in red next to the Current Settings name when there are pending changes to be saved after you have applied default or device group settings. You can also revert to the previously configured settings by clicking **Reset**. The Reset button, which is visible only when you have applied default or group settings to change the current device settings, but have not yet submitted the changes.

If you try to leave this window without saving the modified settings, a dialog box with a warning message prompts you to submit the changes.

Note This dialog box is displayed only if you are using the Internet Explorer browser.

To enable and configure transaction logging from the CLI, use the **transaction-logs** global configuration command.

Transaction Logs

TFO transaction logs are maintained in the local disk in the /local1/logs/tfo directory. Video (Windows media) logs are maintained in the /local1/logs/wmt/wms-90 directory.

When you enable transaction logging, you can specify the interval at which the working log should be archived, by moving the data to an archive log. The archive log files are located on the local disk in the local/local1/logs/working.log directory.

Because multiple archive files are saved, the filename includes the time stamp of when the file was archived. Because the files can be exported to an FTP or SFTP server, the filename also contains the IP address of this WAAS device.

The archive filenames for TFO transactions use this format:

tfo_IPADDRESS_YYYYMMDD_HHMMSS.txt.

The archive filenames for Windows media transactions use this format:

wms_90_IPADDRESS_YYYYMMDD_HHMMSS.txt.

The transaction log format is documented in Appendix B, “Transaction Log Format.”

Viewing the System Message Log

Using the system message log feature of the WAAS Central Manager GUI, you can view information about events that have occurred in your WAAS network. The WAAS Central Manager logs the messages from registered devices with a severity level of *warning*, *error*, or *fatal*.

To view logged information pertaining to your WAAS network, follow these steps:

Step 1 From the WAAS Central Manager menu, choose **Admin > Logs > System Messages**. The System Message Log window appears.

Note If no name is available for a node, “Unavailable” is displayed. This situation might occur if a node has been deleted or has been reregistered with the WAAS software.

Step 2 (Optional) Choose **Quick Filter** from the Show drop-down list, and enter a value in one or more fields to filter the log to include only the entries with the specified values.

Step 3 (Optional) Truncate the message log to ensure that not as many messages appear in the table, by completing the following steps:

a. Click the **Truncate** icon in the taskbar. The Truncate System Message Log pane appears.

b. Choose one of the following options:

- **Size Truncation**—Limits the messages in the log to the number you specify. The log uses a first in, first out process to remove old messages once the log reaches the specified number.
- **Date Truncation**—Limits the messages in the log to the number of days you specify.
- **Message Truncation**—Removes messages that match the specified pattern from the log.

c. Click **OK** after you have finished specifying the truncation parameters.

Viewing the Audit Trail Log

The WAAS Central Manager logs user activity in the system. The only activities that are logged are those activities that change the WAAS network. This feature provides accountability for users' actions by describing the time and action of the task. Logged activities include the following:

- Creation of WAAS network entities
- Modification and deletion of WAAS network entities
- System configurations
- Clearing the audit log

To view audit trail logs, follow these steps:

Step 1 From the WAAS Central Manager menu, choose **Admin > Logs > Audit Trail Logs**.

The Audit Log window appears. All the logged activities in the WAAS Central Manager are listed by user, the IP address of the machine that was used, date and time, and operation that was logged.

Step 2 (Optional) Choose **Quick Filter** from the Show drop-down list, and enter a value in one or more fields to filter the log to include only the entries with the specified values.

Viewing a Device Log

To view information about events that have occurred on a specific device in your WAAS network, use the system message log feature that is available in the WAAS Central Manager GUI.

To view the events that have occurred on your entire WAAS network, see Viewing the System Message Log.

To view the logged information for a WAAS device, follow these steps:

Step 1 From the WAAS Central Manager menu, choose **Devices** > *device-name*.

Step 2 Choose **Admin > Logs > Device Logs**. The Device Log window appears.

Step 3 (Optional) Choose **Quick Filter** from the Show drop-down list, and enter a value in one or more fields to filter the log to include only the entries with the specified values.

CLI Commands for Verifying and Viewing Logs and System Image

- **Verify the WAAS image**—Use the **show version** command to display the version of the software image that is currently running in your WAAS device. This command also displays information including device model and WAE uptime.

- **Verify no pending software**—Use the **show version pending** command to verify that there is no pending software upgrade (waiting for a device reboot).
- **Verify WAAS error logging**—General system error WAAS logging to the disk file /local1/syslog.txt is enabled by default. Use the **show logging** command to verify that logging is enabled.
- **Enable console logging**—Use the **(config) logging console enable** command to enable logging to the console. You can set the following logging priority levels: Alert (Priority 1), Critical (Priority 2), Error (Priority 3), Warning (Priority 4), Notice (Priority 5), Information (Priority 6), and Debug (Priority 7).

Note Setting a logging priority to Levels 1-4 can be CPU-intensive, and can generate a large amount of output.

- **Navigating and viewing log files**—The following directories are used for WAAS log files:
  - **/local1**—Root directory for all log files and location of syslog.txt
  - **/local1/logs**—Service log files (admin and transaction logs)
  - **/local1/errorlog**—Service log files (debug logs)
  - **/local1/errorlog/cifs**—CIFS internal log files (for WAAS versions earlier than Version 6.x)
  - **/local1/core_dir**—Process core dump files

  Use the following commands to navigate and view these log files:
  - **cd**
  - **pwd**
  - **dir**
  - **type-tail** *filename line* **follow**
  - **find-pattern**

Using Diagnostic Tests

This section includes the following topics:

- Device Diagnostics Using the Central Manager
- Device Diagnostics Using the CLI
- Akamai Connect Diagnostics Using the Central Manager

Device Diagnostics Using the Central Manager

The WAAS Central Manager includes a troubleshooting and diagnostic reporting facility.

To perform diagnostic tests, follow these steps:

Step 1 From the WAAS Central Manager menu, choose **Devices** > *device-name* (or **Device Groups** > *device-group-name*).

Step 2 Choose **Monitor** > **Tools** > **Diagnostics Tests**. The Diagnostic Tool window appears.

Step 3 Check the check box next to each diagnostic test you want to run, or check the top check box, Test, to run all tests. The following tests are available:

- Device Operation—Checks the device's status and the presence of coredump files or alarms of major or critical severity.
- Basic Configuration—Checks the device's basic network configuration.
- Basic Connectivity—Checks the device's connectivity to configured external devices (DNS, authentication, NTP servers, and so forth).
- Physical Interface—Checks the configuration and operation of the device's physical interfaces.

Note A Virtual Interface test is available for vWAAS devices.

- Configuration Security—Checks the running configuration for potentially malicious (cross-site scripting [XSS]) entries.
- Traffic Optimization—Checks the TFO configuration and operation.
- WCCP Configuration and Operation—Checks the configuration and operation of WCCP traffic interception.
- Inline configuration and operation—Checks the configuration and operation of inline group interfaces.

Note The inline configuration and operation test is not available for vWAAS devices.

Step 4 Click **Run**.

Step 5 View the test results in the lower part of the window.

Note If any of the tests fail, error messages describe the problem and provide recommended solutions.

You can run the same diagnostic tests again and refresh the results by clicking the **Refresh** icon in the taskbar.

To print the results, click the **Print** icon in the taskbar.

Device Diagnostics Using the CLI

Use the **test** EXEC command to perform diagnostic and connectivity tests.

Use network-level tools to intercept and analyze packets as they pass through your network. Two of these tools are TCPdump and Tethereal, which you can access from the CLI by using the **tcpdump** and **tethereal** EXEC commands.

The WAAS device also supports multiple debugging modes, which can be reached with the **debug** EXEC command. These modes allow you to troubleshoot problems from configuration errors to print spooler problems. We recommend that you use the **debug** command only at the direction of Cisco Technical Assistance Center (TAC).

The output associated with the **debug** command is written to either the syslog file in /local1/syslog.txt or the debug log associated with the module in the file /local1/errorlog/*module_name*-errorlog.current file.

The output associated with the **debug accelerator** *name module* command for an application accelerator is written to the file ao-errorlog.current*name*, where *name* is the accelerator name. The accelerator information manager debug output is written to the aoim-errorlog.current file.

The debug log file associated with a module will be rotated to a backup file when the current file reaches its maximum size. The backup files are named as follows: *name*-errorlog.*#*, where # is the backup file number.

For **debug** commands, system logging must be enabled. The command that enables logging, **logging disk enable**, which is a global configuration command, is enabled by default.

If a **debug** command module uses the syslog for debug output, the **logging disk priority debug** global configuration command must be configured (the default is **logging disk priority notice**).

If a **debug** command module uses the debug log for output, the output can be filtered based on a priority-level configuration for the four different levels of debug log output:

- For filtering of critical debug messages only, use the global configuration command: **logging disk priority critical**.
- For filtering of critical and error-level debug messages, use the global configuration command: **logging disk priority error**.
- For filtering of critical, error, and trace debug level debug messages, use the global configuration command: **logging disk priority debug**.
- For seeing all debug log messages, including critical, error, trace and detail messages, use the following global configuration command: **logging disk priority detail**.

Regardless of the priority-level configuration, syslog messages at the LOG_ERROR or higher severity will be automatically written to the debug log associated with a module.

For more details on these CLI commands, see *Cisco Wide Area Application Services Command Reference*.

Akamai Connect Diagnostics Using the Central Manager

For Cisco WAAS devices with Akamai Connect, the Akamai Diagnostics screen (Figure 16-5) provides status information for the Akamai Connect license and Akamai Connect service, and enables you to unregister or synchronize selected devices.

To use Akamai Diagnostics, follow these steps:

Step 1 From the WAAS Central Manager menu, choose **Home > Monitor > Troubleshoot > Akamai Diagnostics**.

The Akamai Diagnostics screen appears (Figure 16-5).

Figure 16-5 Akamai Diagnostics Screen

Step 2 The upper section of the Akamai Diagnostics screen shows the Akamai Connect License status (Step 3) and the Akamai registration service status (Step 4).

Step 3 Click the *Akamai Connect License* **Details** button to display a dialog box of additional information:

The upper half of the dialog box provides details on the Akamai API credentials used by the WAAS Central Manager for this license (including API host, client ID, and customer ID).

The lower half of the dialog box shows test information, with the message "Below are results of previous test. Please click 'Test" button to get up-to-date results."

a. Click **Test** to test the connection to the API server.

b. A Device Registration Status table listing is displayed, showing the total number of devices, and with columns displaying each WAAS Device, Akamai ID, Akamai Device Status (ActivationInProgress or Active), and Akamai Operational Status (Disconnected, Connected, or Running).

Step 4 Click the *Akamai Registration Service Status* **Details** button to display a dialog box that shows additional status information (including external HTTP proxy, last synchronization with Akamai, number of pending operations, and number of API errors).

a. At the Akamai Registration Service Status dialog box, check the **Enable debugging Akamai API calls** check box to enable debugging of Akamai API calls.

The Device Registration Service Status dialog box displays an API error log with the total number of API errors, and a table listing with columns labeled When, Device, Operation (such as Refresh All Devices), and Error Message (such as Read timed out(HTTP status code -1)).

Step 5 The lower section of the Akamai Diagnostics screen is a table listing of WAAS devices with Akamai Connect, with columns for WAAS Device, Akamai Device Status (ActivationInProgress or Active), Operational Status (Disconnected, Connected, or Running), and Connectivity to Akamai (Disconnected, Activating, or Connected).

The table heading provides two buttons: **Unregister** (Step 6) and **Synchronize** (Step 7).

Step 6 To unregister a device from this table listing:

a. Select the device(s).

b. Click the **Unregister** button in the table heading.

The **Unregister** button triggers the removal of the device record on the Akamai server, and invalidates the entitlement key used by the Cache Engine to talk with Akamai Connect devices. The unregistered device can continue to function with transparent caching benefits, but it will not utilize Akamai Connected Cache or OTT caching benefits.

c. When you click **Unregister**, the following warning message is displayed: "De-registering device(s) would prevent Akamai Connected Cache and OTT features from working on devices that have these features enabled. Please confirm de-registration of selected device(s)."

d. Click **OK** to de-register to the selected device(s) or click **Cancel** to exit the procedure without de-registering the selected device(s).

Step 7 Click the **Synchronize** button in the table heading.

a. Synchronization between the Akamai server and the WAAS Central Manager occurs in specified time intervals automatically. The **Synchronize** button enables you to trigger synchronization between the Akamai server and all Akamai-registered WAAS devices,

b. When you click **Synchronize**, it communicates with the Akamai server for the latest updates of all devices registered with the Central Manager, and the status of these devices is updated accordingly.

Note the following operating considerations when using the Synchronize button:

- The **Synchronize** button applies to all Akamai-enabled devices; it is not specific to a particular device update.
- You can check the last synchronization time from the Akamai Registration Service Status Details button, described in Step 4.

Using the Kernel Debugger

The WAAS Central Manager GUI allows you to enable or disable access to the kernel debugger (kdb). After being enabled, the kernel debugger is automatically activated when kernel problems occur.

To enable the kernel debugger, follow these steps:

Step 1 From the WAAS Central Manager menu, choose **Devices** > *device-name* (or **Device Groups** > *device-group-name*).

Step 2 Choose **Monitor** > **Tools** > **Kernel Debugger**. The Kernel Debugger window appears.

Step 3 Check the **Enable** check box to enable the kernel debugger, and click **Submit**. (By default, this option is disabled.)

Using WAAS TCP Traceroute

The WAAS TCP Traceroute tool can help you troubleshoot network and connection issues, including asymmetric paths. You can use it to find a list of WAAS nodes between the client and the server, and the configured and applied policies for a connection. From the Central Manager, you can choose any device in your WAAS network from which to run the traceroute.

To use the WAAS Central Manager TCP Traceroute tool, follow these steps:

Step 1 From the WAAS Central Manager menu, choose **Monitor > Troubleshoot > WAAS Tcptraceroute**.

Alternatively, you can choose a device first and then choose this menu item to run the traceroute from that device.

Step 2 From the WAAS Node drop-down list, choose a WAAS device from which to run the traceroute. (This item does not appear if you are in the device listing.)

Step 3 In the Destination IP and Destination Port fields, enter the IP address and port of the destination for which you want to run the traceroute

Step 4 Click **Run TCPTraceroute** to display the results.

WAAS nodes in the traced path are displayed in the table below the fields. From the Show drop-down list, choose a filter setting to filter the devices, as needed. You can use a quick filter to filter any value, or show all devices.

You can view traceroute information from the CLI by using the **waas-tcptrace** EXEC command.

Another troubleshooting tool that you can use to trace connections on a WAAS appliance ANC is the Connection Trace tool. For details, see AppNav Connection Tracing in Chapter 4, “Configuring AppNav.”

Verifying WAAS Physical Connectivity

This section has the following topics:

- Verifying Physical Connectivity Between Peer WAAS Devices
- Verifying Physical Connectivity Between WAAS Data Center and Application Server Hosts

Verifying Physical Connectivity Between Peer WAAS Devices

To verify physical connectivity between peer WAAS devices, follow these steps:

Step 1 Check all cable connections on the switch or router that may impact the WAAS device.

Step 2 Use the **ping** command to send an ICMP Echo request to the peer WAE. For example:

```
WAE# ping 10.1.1.2 172.19.131.189
PING 172.19.131.189 (172.19.131.189) from 10.1.1.21 : 56(84) bytes of data.
64 bytes from 172.19.131.189: icmp_seq=0 ttl=249 time=613 usec
64 bytes from 172.19.131.189: icmp_seq=1 ttl=249 time=485 usec
64 bytes from 172.19.131.189: icmp_seq=2 ttl=249 time=494 usec
64 bytes from 172.19.131.189: icmp_seq=3 ttl=249 time=510 usec
64 bytes from 172.19.131.189: icmp_seq=4 ttl=249 time=493 usec

--- 172.19.131.189 ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max/mdev = 0.485/0.519/0.613/0.047 ms
```

Step 3 If a device is one hop away and you are unable to reach the device, then ping the intermediary gateway. If the gateway is not reachable, use the **show ip routes** command to verify that the correct route is displayed.

Step 4 If necessary, enter a static route for the gateway.

Note Firewalls may block ICMP traffic, and ICMP traffic does not follow the WCCP redirection path. Therefore, using the ping command does not verify redirection or acceleration. As an alternative way to verify redirection or acceleration, we recommend that you use a third-party tool that performs a TCP-based ping.

Verifying Physical Connectivity Between WAAS Data Center and Application Server Hosts

The procedure for verifying physical connectivity between WAAS data center and application server hosts is the same procedure as described in Verifying Physical Connectivity Between Peer WAAS Devices.

Contacting Cisco Technical Support

If you are unable to resolve a problem after using the troubleshooting suggestions in this chapter, contact the Cisco Technical Assistance Center (TAC) for assistance and further instructions. Before you call, have the following information ready to help your TAC engineer assist you as quickly as possible:

- Date that you received the WAAS hardware
- Chassis serial number
- Type of software and release number (if possible, enter the show version command)
- Maintenance agreement or warranty information
- A good problem description including:
  - What is the problem and what are the user visible symptoms?
  - Where and when it occurs
  - Error messages, alerts, and alarms seen
  - Steps to duplicate the problem
- Brief explanation of the steps that you have already taken to isolate and resolve the problem
- The diagnostic test output (see the "Running Diagnostics" section)
- A Central Manager database backup (use the cms database backup command)
- Information gathered in the "Gathering WAAS Troubleshooting Information" section.
- Topology diagrams, including network/wiring diagrams and logical diagrams
- Any other evidence of the problem such as packet captures, transaction logs, core files, WCCP show command output from routers/switches and WAEs, and other log files.

You can contact support in these ways:

- Contact TAC
- Contact the Small Business Support Center (SBSC)