CHAPTER 15

Monitoring and Troubleshooting Your WAAS Network

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

Note Throughout this chapter, the term WAAS device is used to refer collectively to the WAAS Central Managers and WAEs in your network. The term WAE refers to WAE appliances and WAE Network Modules (the NME-WAE family of devices).

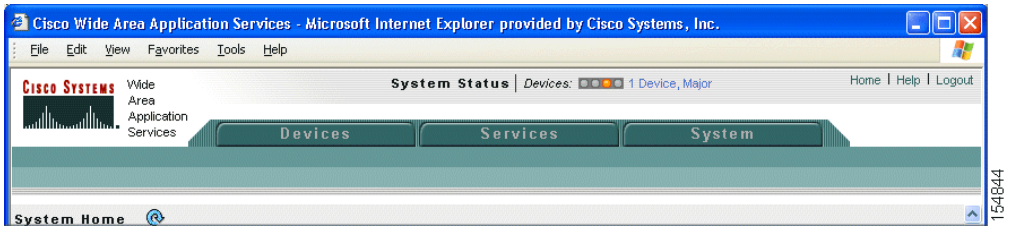
This chapter contains the following sections:

- Using the System Status Bar, page 15-2
- Using the show and clear Commands from the WAAS Central Manager GUI, page 15-4
- Viewing Device Information, page 15-5
- Configuring System Logging, page 15-8
- Configuring Transaction Logging, page 15-10
- Viewing the System Message Log, page 15-15
- Viewing the Audit Trail Log, page 15-17
- Viewing the Device Log, page 15-18
- Using the Traffic Statistics Report to Monitor Applications, page 15-18
- Viewing CPU Utilization for a Device, page 15-27
- Enabling the Kernel Debugger, page 15-27
- Troubleshooting Using the CLI, page 15-27

Using the System Status Bar

The WAAS Central Manager GUI displays the system status above the navigation tabs in every window. The system status bar presents the overall device and content health of the system. You can use this feature to monitor devices in your WAAS network. The system status bar helps you immediately identify any problems on the network, allowing you to act and respond to problems quickly. (See Figure 15-1.)

Figure 15-1 System Status Bar

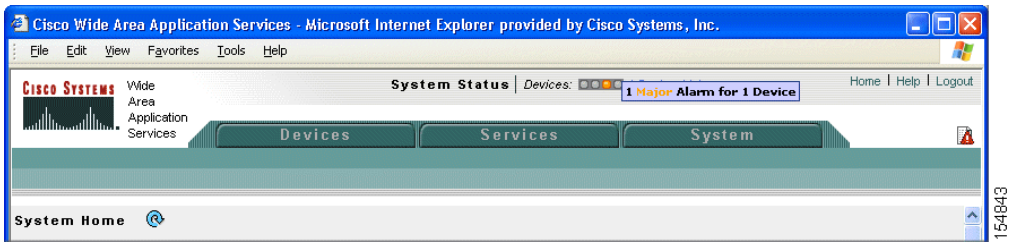


The system status reporting mechanism uses four alarm lights to identify problems that need to be resolved. Each light represents a different alarm level, as follows:

- Green—No alarms (the system is in excellent health)
- Yellow—Minor alarms
- Orange—Major alarms
- Red—Critical alarms

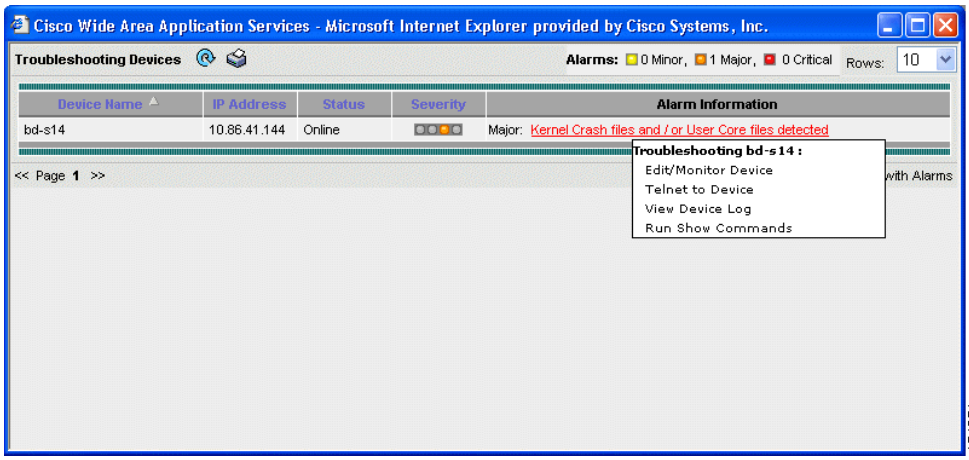
When you roll your mouse over an alarm light in the system status bar, a popup message provides further details about the device. (See Figure 15-2.)

Figure 15-2 Status Details



When you click the alarm light, the Troubleshooting Devices window appears, listing the individual devices that need attention. (See Figure 15-3.) When you roll your mouse over an item under the Alarm Information column in the Troubleshooting Devices window, a contextual popup menu appears. The popup menu provides links to the troubleshooting and monitoring windows in the WAAS Central Manager GUI. For more information on using the Troubleshooting Devices window, see the "Troubleshooting Devices Using the System Status Bar" section on page 15-4.

Figure 15-3 Troubleshooting Devices Window



This section contains the following topics:

- Device Alarms, page 15-3
- Troubleshooting Devices Using the System Status Bar, page 15-4

Device Alarms

Device alarms are associated with device objects and pertain to applications and services running on your WAEs. 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 15-1 describes the various device alarms that can appear.

Table 15-1 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.
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 is not interoperable with the WAAS Central Manager because it has an earlier software version.

Troubleshooting Devices Using the System Status Bar

To troubleshoot a device from the system status bar, follow these steps:

Step 1 In the system status bar, click the Devices alarm light or click the alarm message next to the Devices alarm light panel. The Troubleshooting Devices window pops up as a separate window. (See Figure 15-3 on page 15-3.)

Step 2 In the Alarm Information column, hold your mouse over the alarm message until the Troubleshooting tools menu appears.

Step 3 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 15-2 describes the tools available for all device alarms.

Table 15-2 Troubleshooting Tools for Device Alarms

Item	Navigation	Description
Edit/Monitor Device	Device Home	Displays device home window for configuration.
Telnet to Device	Opens a Telnet window	Initiates a Telnet session using the device IP address.
View Device Logs	**Devices > Monitoring > Logs**	Displays system message logs filtered for this device.
Run Show Commands	**Devices > Monitoring > Show/Clear Commands > Show Commands**	Displays device **show** command tool. For more information, see the "Using the show and clear Commands from the WAAS Central Manager GUI" section on page 15-4.

Using the show and clear Commands from the WAAS Central Manager GUI

To use the WAAS Central Manager GUI **show** and **clear** command tool, follow these steps:

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

Step 2 Click the **Edit** icon next to the device for which you want to issue a **show** or **clear** command.

Step 3 Click **Show Advanced** to display all the menu items in the Contents pane.

Step 4 From Contents pane, choose **Monitoring > Show/Clear Commands** and then click either **Show Commands** or **Clear Commands**.

Step 5 From the drop-down list, choose a **show** or **clear** command.

Step 6 Enter arguments for the command, if any.

Step 7 Click **Submit** to display the command output.

A window appears, displaying the command output for that device.

You can also use the **show** EXEC commands from the CLI. For more information, see the *Cisco Wide Area Application Services Command Reference*.

Viewing Device Information

The WAAS Central Manager GUI allows you to view basic and detailed information about a device from the following two windows:

- Devices Window—Displays a list of all the devices in your WAAS network along with basic information about each device such as the device status and the current software version installed on the device.
- Device Home Window—Displays detailed information about a specific device, such as the installed software version and whether the device is online or offline.

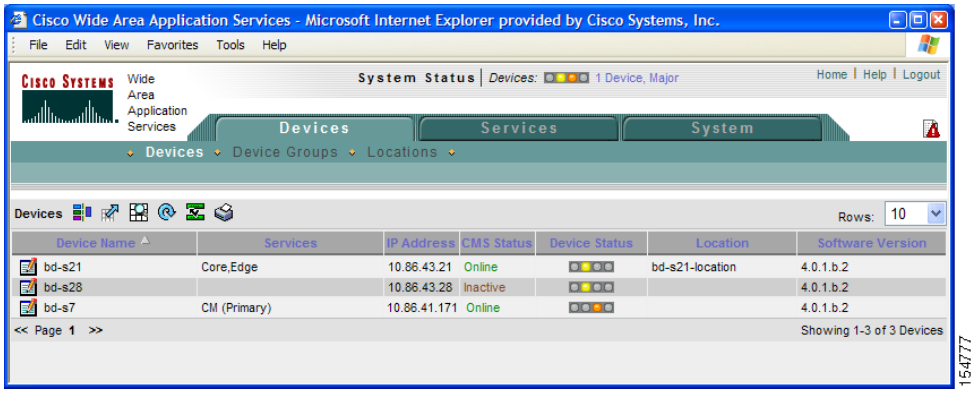
Each window is explained in the sections that follow.

Devices Window

The Devices window lists all the WAAS devices that are registered with the WAAS Central Manager. To view this list, choose **Devices > Devices** in the WAAS Central Manager GUI.

Figure 15-4 shows an example of the Devices window.

Figure 15-4 Devices Window



This window displays the following information about each device:

- Services enabled on the device. See Table 15-3 for a description on these services.
- IP address of the device.
- CMS Status (online, offline, pending, inactive). For more information about status, see the "Device Alarms" section on page 15-3.
- Device Status. For more information about the status indicator, see the "Using the System Status Bar" section on page 15-2.

- Location associated with the device. For more information about locations, see Chapter 3, "Using Device Groups and Device Locations."
- Software version installed and running on the device.

Table 15-3 Service Descriptions

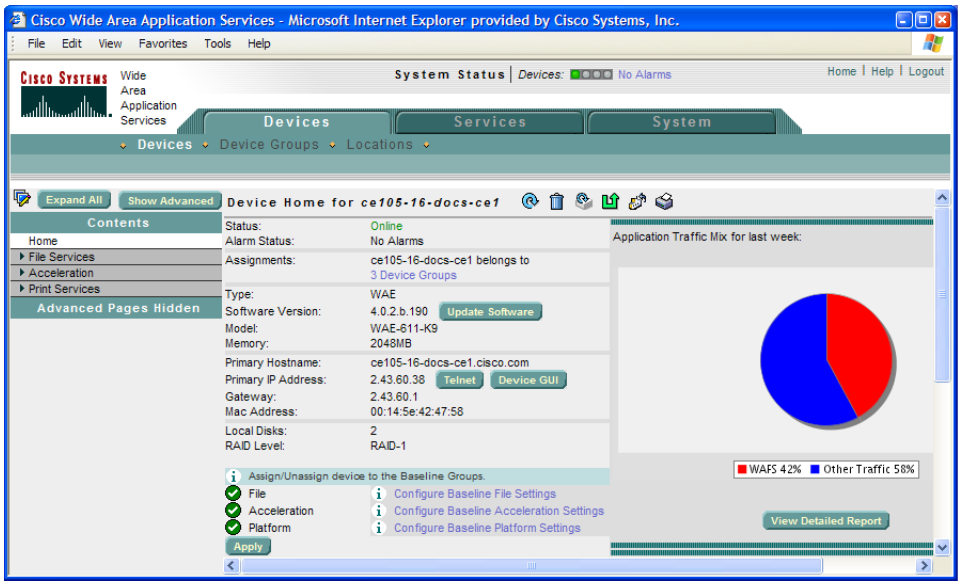
Service	Description
Edge	The device has been enabled with Edge services so it can accelerate data stored on a remote file server. For information on enabling Edge services, see Chapter 11, "Configuring WAFS."
Core	The device has been enabled with Core services so it can accelerate data stored on a remote file server. For information on enabling Core services, see Chapter 11, "Configuring WAFS."
CM (Primary)	The device has been enabled as the primary WAAS Central Manager. For information on primary and standby Central Manager devices, see the "Switching a WAAS Central Manager from Standby to Primary" section on page 14-20.
CM (Standby)	The device has been enabled as a standby WAAS Central Manager. For information on primary and standby Central Manager devices, see the "Switching a WAAS Central Manager from Standby to Primary" section on page 14-20.
Print	The device has been enabled with print services so it can act as a print server to branch office clients. For information on setting up a print server, see Chapter 13, "Configuring and Managing WAAS Print Services."

Device Home Window

The Device Home window provides detailed information about a WAAS device such as the installed software version and whether the device is online or offline. (See Figure 15-5.)

To access the Device Home window, go to **Devices > Devices** and click the **Edit** icon next to the device that you want to view.

Figure 15-5 Device Home Window



From the Device Home window you can perform the following tasks:

- View basic details such as whether the device is online, the device's IP address and hostname, the software version running on the device, and the amount of memory installed in the device.

Note If the device you are viewing is running software version 4.0.1, the amount of memory that is installed is not shown because the device does not report it.

- View the device groups that the device belongs to. For more information about device groups, see Chapter 3, "Using Device Groups and Device Locations."
- Click **Update Software** to update the software on the device. For more information, see Chapter 14, "Maintaining Your WAAS System."
- Click **Telnet** to establish a Telnet session into the device and issue CLI commands.
- Click **Device GUI** to open the WAE Device Manager. For more information on managing a device using this GUI, see Chapter 10, "Using the WAE Device Manager GUI."
- Assign and unassign the device to baseline groups. For more information, see Chapter 3, "Using Device Groups and Device Locations."
- View the Application Traffic Mix chart and the Reduction chart.

  The Application Traffic Mix chart displays the nine applications with the highest percentage of traffic on the device. The Traffic Reduction chart displays the ten applications with the highest percent reduction for this device. The percent calculation includes pass-through traffic.

  To change the report options for these charts, click **View Detailed Report** under the chart. For information, see the "Viewing the Traffic Statistics Report for a Device" section on page 15-19.

Note The Device Home window for the WAAS Central Manager only supports a subset of the tasks listed. For example, the Application Traffic Mix chart and the Reduction chart are not displayed for the WAAS Central Manager because this type of WAAS device does not optimize traffic.

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 on the system file system (sysfs) partition as /local1/syslog.txt.

To enable system logging, follow these steps:

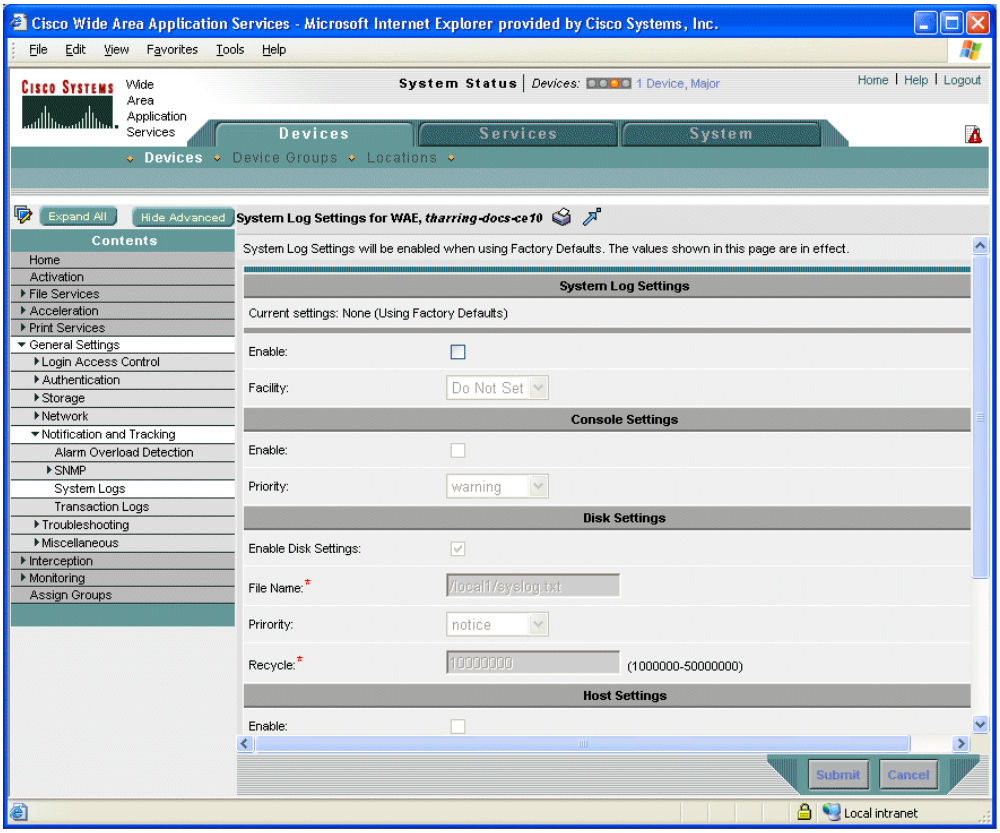
Step 1 From the WAAS Central Manager GUI, choose **Devices > Devices** or **Devices > Device Groups**.

Step 2 Click the **Edit** icon next to the device or device group for which you want to enable system logging. The Contents pane appears on the left.

Step 3 Click **Show Advanced** to display the advanced menu items in the Contents pane.

Step 4 From the Contents pane, choose **General Settings > Notification and Tracking > System Logs**. The System Log Settings window appears. (See Figure 15-6.)

Figure 15-6 System Log Settings Window



Step 5 Under the System Log Settings section, check the **Enable** check box to enable system logging. By default, this option is disabled.

Step 6 From the Facility drop-down list, choose the appropriate facility.

Step 7 Enable system log files to be sent to the console, by following these steps:

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 15-4 on page 15-10 for a list of priority levels.)

Step 8 Enable syslog files to be sent to disk, by following these steps:

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

b. In the File Name field, enter a path and a filename where the syslog files will be stored on 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 15-4 on page 15-10 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 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 at most 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 configured in the File Name field (or by using the **logging disk filename** command).

Step 9 Enable syslog files to be sent to a host, by following these steps:

a. In the Host Settings section, check the **Enable** check box. You can configure up to four hosts to which syslog messages can be sent. For more information, see the "Multiple Hosts for System Logging" section on page 15-10."

b. In the Hostname field, enter a hostname or IP address of the remote syslog host. Specify up to three more remote syslog hosts in the Hostname fields 2 through 4. You must specify at least one hostname if you have enabled system logging to a host.

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 15-4 for a list of priority levels.)

d. 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.

e. In the Rate 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 10 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, page 15-10
- Multiple Hosts for System Logging, page 15-10

Priority Levels

Table 15-4 lists the different priority levels of detail to send to the recipient of the syslog messages for a corresponding event.

Table 15-4 System Logging Priority Levels and Descriptions

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

If you want 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 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) to control the amount of bandwidth used by syslog messages.

Configuring Transaction Logging

This section contains the following topics:

- Enabling Transaction Logging, page 15-11
- Transaction Logs, page 15-13
- Real-Time Transaction Logging, page 15-14

Enabling Transaction Logging

To enable transaction logging, follow these steps:

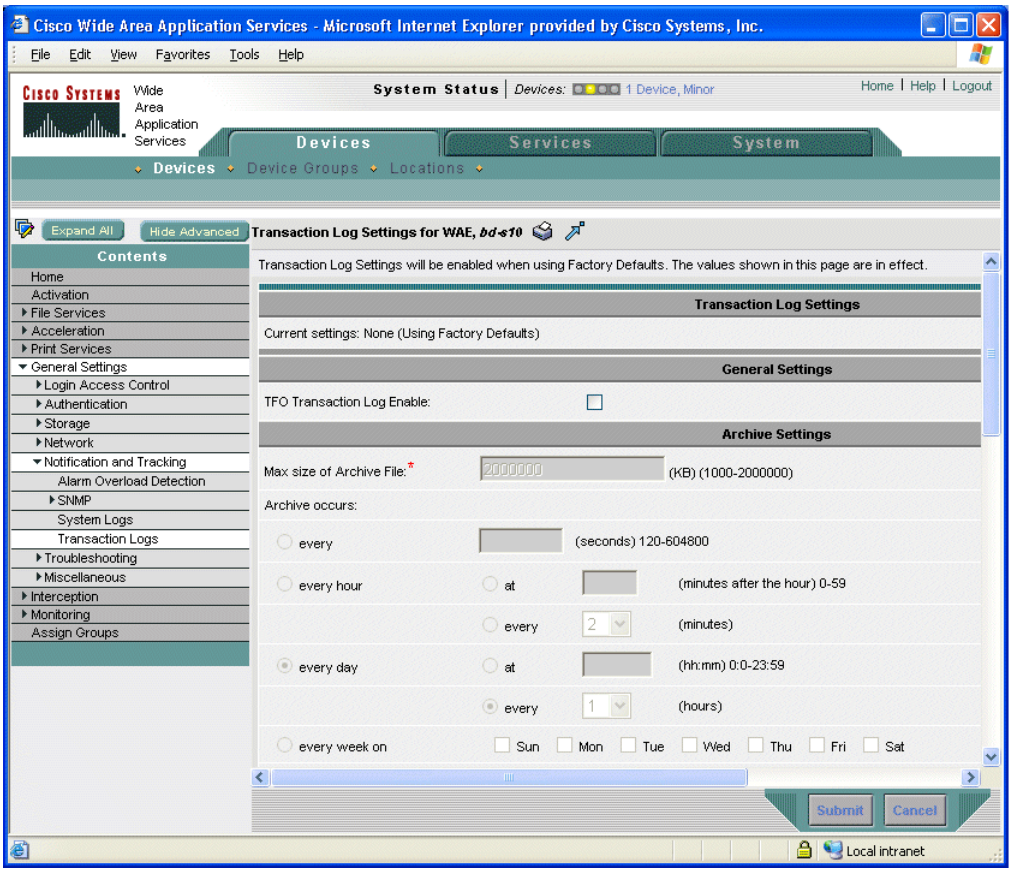
Step 1 From the WAAS Central Manager GUI, choose **Devices > Devices** or **Devices > Device Groups**.

Step 2 Click the **Edit** icon next to the device or device group for which you want to enable system logging. The Device Home window or the Modifying Device Group window appears.

Step 3 Click **Show Advanced** to display the advanced menu items in the Contents pane.

Step 4 From the Contents pane, choose **General Settings > Notification and Tracking > Transaction Logs**. The Transaction Log Settings window appears. (See Figure 15-7.)

Figure 15-7 Transaction Log Settings Window



Step 5 Under the General Settings heading, check the **TFO Transaction Log Enable** check box to enable transaction logging.

The fields on the window become active.

Step 6 Under the Archive Settings heading, 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 archived 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 7 Configure the fields in the Export Settings section to export the transaction log file to an FTP server.

Table 15-5 describes the fields in the Export Settings section.

Table 15-5 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. • **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, place a check in the SFTP check box.

Step 8 Configure the settings in the Logging Settings section to configure real-time transaction logging.

Table 15-6 describes the fields in the Logging Settings section. For more information about real-time transaction logging, see the "Real-Time Transaction Logging" section on page 15-14.

Table 15-6 Logging Settings

GUI Parameter	Function
Enable	Enables real-time transaction logging. You can retain the logging host configuration for transaction logs even if you temporarily disable real-time transaction logging by unchecking the check box. This new logging option applies only to the cache's HTTP transaction log entries. The real-time transaction logging feature is disabled by default.
Facility	Choose the appropriate transaction log facility. This drop-down list is set to an initial value of *Do not set*. This setting denotes that the facility sent to the syslog host will be the facility on the local host that is sending the syslog message. For instance, in the case of the transaction logging module that sends the real-time transaction log message, the facility is the "user" facility.
Enable Host Settings	Enables the transaction log files to be sent to a remote syslog host.

Table 15-6 Logging Settings (continued)

GUI Parameter	Function
Hostname	The hostname or IP address of the remote syslog server to which transaction logs must be sent. No remote syslog server is specified by default.
Port	The destination port on the remote syslog host to which the WAAS device should send the transaction log files. The default port number is 514. This port is a well-known port for system logging.
Rate Limit	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 (rate-limit is set to 0), and by default all syslog messages are sent to all of the configured syslog hosts. The range is 1 to 10,000 messages per second.

Step 9 Click **Submit**.

A "Click Submit to Save" message appears in red next to the Current Settings line 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 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 warning dialog box prompts you to submit the changes. This dialog box only appears if you are using the Internet Explorer browser.

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

Transaction Logs

Depending upon where the sysfs is mounted, transactions are logged to a working log on the local disk in one of these files:

- /local1/logs/working.log
- /local2/logs/working.log

When you enable transaction logging, you can specify the interval at which the working log should be cleared by moving the data to an archive log. The archive log files are located on the local disk in the directory /local1/logs/ or /local2/logs/, depending upon where the sysfs is mounted.

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

The archive file name use this format:

celog_IPADDRESS_YYYYMMDD_HHMMSS.txt.

Real-Time Transaction Logging

You can monitor transaction logs in real-time for particular errors such as authentication errors. By sending HTTP transaction log messages to a remote syslog server, you can monitor the remote syslog server for HTTP request authentication failures in real-time. This real-time transaction log feature allows you to monitor transaction logs in real-time for particular errors such as HTTP request authentication errors. The existing transaction logging to the local file system remains unchanged.

For this purpose, you must configure the WAAS device to send transaction log messages to a remote syslog server using UDP as the transport protocol. Because UDP is an unreliable transport protocol, message transport to remote syslog host is not reliable and you must monitor the syslog messages received at the remote syslog server. You can limit the rate at which the transaction logging module is allowed to send messages to the remote syslog server. The format of the syslog message is in standard syslog message format with the transaction log message as the payload of the syslog message.

Real-time transaction logging to a remote syslog server uses the standard syslog message format with the message payload as the transaction log entry. A new syslog error identifier is defined for this type of real-time transaction log message. You can configure a WAAS device to send transaction log messages in real-time to one remote syslog host. The message format of the transaction log entry to the remote syslog host is the same as in the transaction log file and prepended with Cisco's standard syslog header information.

The following is an example of the format of the real-time syslog message sent from the transaction logging module (WAAS device) to the remote syslog host:

fac-pri Apr 22 20:10:46 *wae-host cache*: %WAAS-TRNSLG-6-460012: *translog formatted msg*

The fields in the message are described as follows:

- *fac-pri* denotes the facility parameter and priority for transaction log messages encoded (as in standard syslog format) as a 32-bit decimal value between 0 and 1023 (0x0000 and 0x03FF). The least significant three bits indicate priority (0 to 7) and the next least significant seven bits indicate facility (0 to 127).

  The facility parameter used by the transaction logging module when a real-time transaction log message is logged to the remote syslog host is *user*. The same facility is sent to the remote syslog host unless you configure a different facility parameter for transaction logging. The priority field is always set to LOG_INFO for real-time transaction log messages.

  In the above example, the default value of *fac-pri* is 14 (0x000E) where facility = user (LOG_USER (1)) and priority = LOG_INFO (6).
- The next field in the message is the date, which follows the format as shown in the above example.
- *wae-host* is the hostname or IP of the WAAS device that is sending the message.
- *cache* is the name of the process on the WAAS device that is sending the message.
- %WAAS-TRNSLG-6-460012 is the Cisco standard formatted syslog header on the WAAS device for a real-time transaction log message. This identifier indicates a priority level of 6, which indicates informational messages.

Note The WAAS device system syslog messages report communication errors with the remote syslog host that is configured for transaction logging. These syslog messages are in the error message range: %WAAS-TRNSLG-6-460013 to %WAAS-TRNSLG-3-460016. The last error message (%WAAS-TRNSLG-3-460016), shows level "3" (for error-level messages) instead of "6" (for information-level messages). Information-level messages are reported when messages are dropped due to rate limiting and the number of dropped messages are reported.

- *translog formatted msg* is the transaction log message as it appears in the transaction log file.

Note The total length of the real-time syslog message is 1024 characters. If the actual transaction log entry exceeds this limit, it is truncated.

When the remote syslog server logs this message to a file, the format appears as follows:

Apr 22 20:10:46 *wae-host cache*: %WAAS-TRNSLG-6-460012: *translog formatted msg*

wae-host is the hostname of the WAAS device that sent the real-time transaction log message to the remote syslog server.

The configuration of host settings for transaction logs is identical to the configuration settings for syslog messages except that you need not specify the priority level of the message for real-time transaction logs. All messages are associated with the priority level of 6 (LOG_INFO). You are not required to filter messages based on priority levels.

Viewing the System Message Log

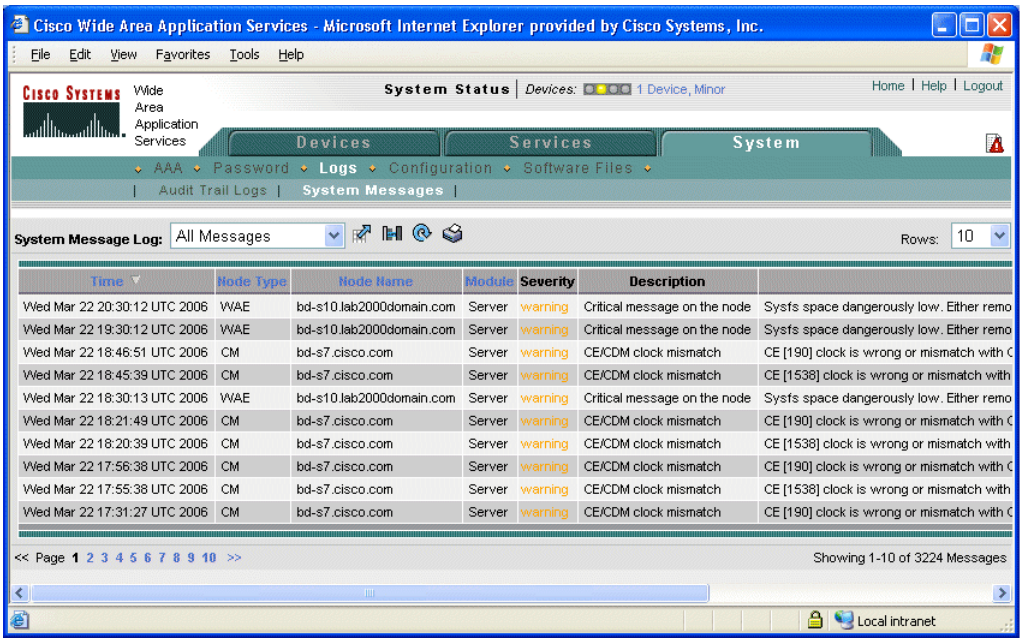
Using the system message log feature of the WAAS Central Manager GUI, you can view information about events that have occurred in your WAAS network.

Note The WAAS Central Manager logs messages only of the severity level “critical” or higher from registered devices.

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

Step 1 From the WAAS Central Manager GUI, choose **System > Logs > System Messages**. The System Message Log window appears. (See Figure 15-8.)

Figure 15-8 System Message Log



Step 2 From the System Message Log drop-down list, choose one of the following types of messages to display:

- All
- CLI
- Critical
- Database

Step 3 (Optional) Click a column heading by node type, node name, module, or message text to sort the messages. By default, messages are listed chronologically.

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

Step 4 (Optional) Truncate the message log so 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 window 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 from the log that match the specified pattern.

c. Click **Submit** when finished specifying the truncation parameters.

Step 5 If you have many event messages, you may need to view multiple pages to view the activity in which you are interested. Click the forward (>>) and back (<<) buttons to move between pages. Alternatively, click the link for a specific page number to jump to that page.

Viewing the Audit Trail Log

The WAAS Central Manager logs user activity in the system. The only activities that are logged are those 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:

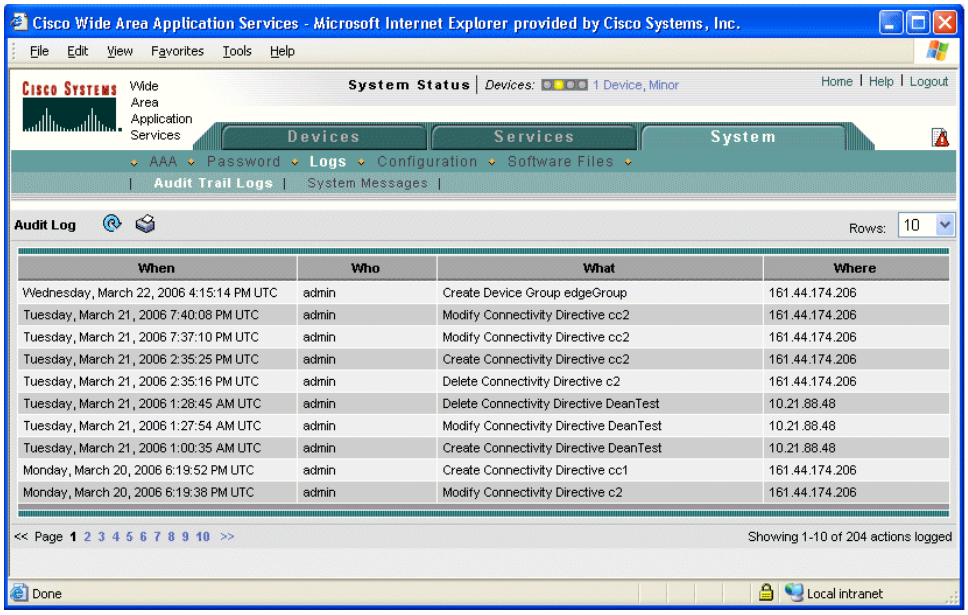
- Creation of WAAS network entities
- Modification and deletion of WAAS network entities
- System configurations

To view audit trail logs, follow these steps:

Step 1 From the WAAS Central Manager GUI, choose **System > Logs > Audit Trail Logs**.

The Audit Log window appears. (See Figure 15-9.) All logged transactions in the WAAS Central Manager are listed by date and time, user, actual transaction that was logged, and the IP address of the machine that was used.

Figure 15-9 Audit Log Window



Step 2 Choose a number from the Rows drop-down list to determine the number of rows that you want to display.

Viewing the Device Log

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

To view events that have occurred on your entire WAAS network, see the "Viewing the System Message Log" section on page 15-15.

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

Step 1 From the WAAS Central Manager GUI, choose **Devices > Devices**. The Devices window appears.

Step 2 Click the **Edit** icon next to the device for which you want to view the system message log details. The Device Home window appears with the Contents pane on the left.

Step 3 Click **Show Advanced** to display all the menu items in the Contents pane.

Step 4 In the Contents pane, choose **Monitoring > Logs**. The System Message Log for Device window appears.

Step 5 Choose the type of messages to be displayed from the System Message Log drop-down list.

You can view the following types of messages in the system log:

- All (default)
- CLI
- Critical
- Database

Step 6 Click a column heading to arrange the messages chronologically by node type, node name, or module. By default, messages are displayed chronologically.

If no name is available for a node because the node has been deleted or reregistered with the Cisco WAAS software, the message displayed is "Unavailable."

Step 7 If you have many event messages, you may need to use the forward (>>) and back (<<) buttons to move between pages. Alternatively, click the link for a specific page number to move to that particular page.

Using the Traffic Statistics Report to Monitor Applications

The Traffic Statistics report provides charts and detailed statistics about the application traffic processed by your WAAS system. You can view this report for an individual WAE or for your entire WAAS network.

Note The clock on each WAE device must be synchronized within half hour of the WAAS Central Manager clock for statistics to be displayed.

This section contains the following topics:

- Viewing the Traffic Statistics Report for a Device, page 15-19
- Viewing the Traffic Statistics Details Report for a Device, page 15-21
- Viewing the System-Wide Traffic Statistics Report, page 15-22
- Charts in the Traffic Statistics Report, page 15-24

Viewing the Traffic Statistics Report for a Device

The WAAS Central Manager GUI allows you to view the Traffic Statistics report for a specific WAE device. This report provides various charts that each show a different view of the application traffic for a specified time period.

To view the Traffic Statistics report for a WAE device, follow these steps:

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

Step 2 Click the **Edit** icon next to the device for which you want to view a report. The Device Home window is displayed.

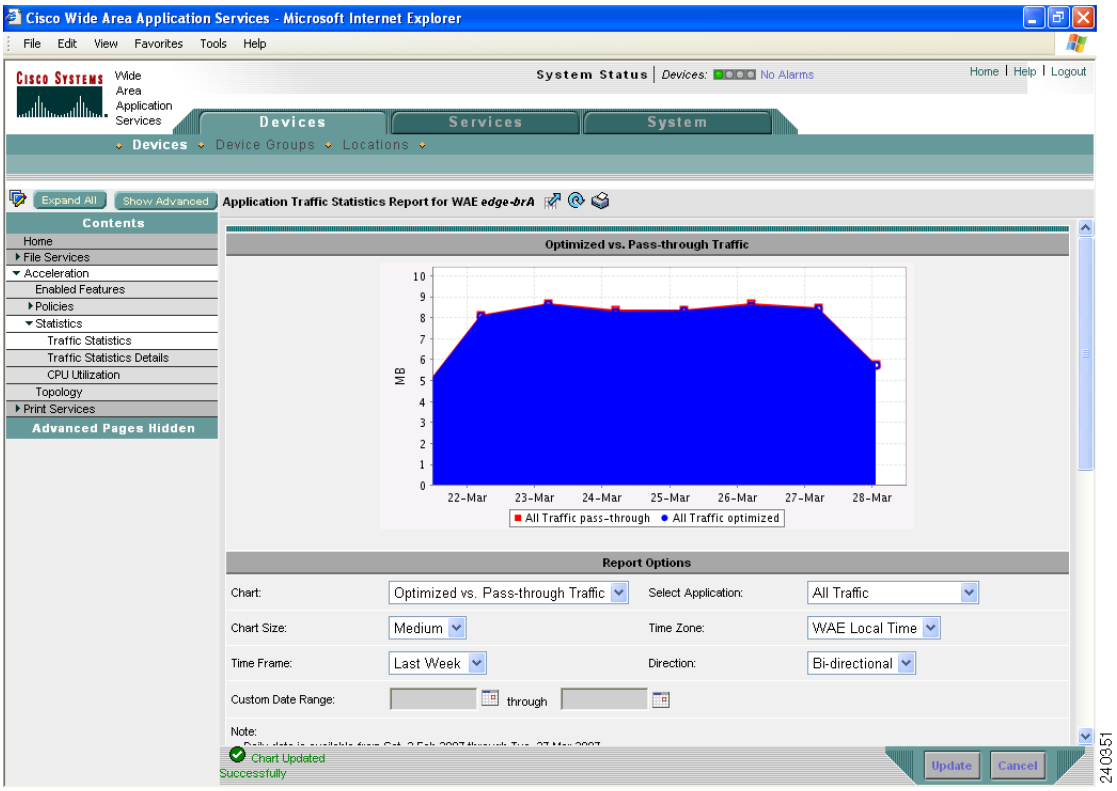
Step 3 From the Contents pane, choose **Acceleration > Statistics > Traffic Statistics**. The Application Traffic Statistics window is displayed.

Alternatively, you can also click **View Detailed Report** on the Device Home window to display the Application Traffic Statistics window.

Step 4 From the Chart drop-down list, choose one of the following chart types:

- **Reduction (incl. pass-through)**—Displays the percent of total traffic that was reduced on the WAE device using the WAAS optimization techniques. This chart includes pass-through traffic in the total results.
- **Reduction (excl. pass-through)**—Displays the percent of total traffic that was reduced on the WAE device using the WAAS optimization techniques. This chart excludes pass-through traffic in the total results.
- **Application Traffic Mix**—Displays the top nine applications with the most traffic on the WAE device.
- **Application Traffic**—Allows you to compare the traffic associated with specific applications to the total traffic processed on the WAE device.
- **Pass-through Traffic Mix**— Displays the most common reason that traffic passed through the WAE device unoptimized. This chart allows you to show traffic statistics for all applications or for one specific application.
- **Pass-through Traffic**—Displays the most common reason that traffic passed through the WAE device unoptimized. This chart allows you to show traffic statistics for multiple applications that you specify.
- **Optimized vs. Pass-through Traffic**—Displays the amount of optimized and pass-through traffic on the WAE device. This chart allows you to show traffic statistics for multiple applications that you specify. The chart in the display is a stacked graph; the pass-through traffic data is indicated by the color red and is shown above the optimized data which is indicated by the color blue. (See Figure 15-10.)

Figure 15-10 Optimized vs. Pass-Through Traffic Graph



Step 5 From the Chart Size drop-down list, choose **Small**, **Medium**, or **Large**.

Step 6 From the Time Zone drop-down list, choose one of the following options:

- **WAE Local Time**—Sets the time zone of the report to the time zone of the WAAS device.
- **CM Local Time (default)**—Sets the time zone of the report to the time zone of the WAAS Central Manager.
- **UTC**—Sets the time zone of the report to UTC.

Note Changing the time-zone does not affect the data plotted on the graph. It only modifies the time-scale displayed to be based on the chosen time-zone.

Step 7 From the Time Frame drop-down list, choose one of the following options:

- **Last Hour**—Displays data for the past hour (in five-minute intervals). You can change this interval using the System.monitoring.collectRate configuration setting described in the "Modifying the Default System Configuration Properties" section on page 9-10.
- **Last Day**—Displays data for the past day (in hourly intervals).
- **Last Week**—Displays data for the past week (in daily intervals).
- **Last Month**—Displays data for the past month (in daily intervals).
- **Custom**—Displays data for the time interval you specify. After choosing this option, enter the start and ending dates for the report in the fields provided. You can also click the calendar icon next to each field to choose dates from a pop-up calendar.

Step 8 From the Direction drop-down list, choose one of the following options:

- **Outbound**—Includes traffic traveling from a client to the WAN through this WAAS device.
- **Inbound**—Includes traffic from the WAN to the client through this WAAS device
- **Bi-directional**—Includes LAN to WAN traffic as well as WAN to LAN traffic traveling through this WAAS device.

The data displayed on the graph and the summary table will be for the chosen direction.

Step 9 Choose the applications to include in the chosen chart. Table 15-7 describes how to choose applications based on the chart type you chose in Step 4.

Table 15-7 Choosing Applications for Various Chart Types

Chart Type	Action
Reduction chart, Application Traffic chart, or Pass-through Traffic chart	Place a check next to each application that you want to include from the list of applications displayed at the bottom of the page.
Application Traffic Mix chart	The report automatically displays the top nine applications with the most traffic. You cannot choose specific applications to include in this report.
Pass-through Traffic Mix chart, or Optimized vs. Pass-through Traffic chart	Use the **Application** drop-down list to choose the application that you want to include in the report. This drop-down list is only available for the Pass-through Traffic Mix and Optimized vs. Pass-through Traffic reports. To include all applications, choose **All Traffic** from the **Application** drop-down list.

Step 10 Click **Update**. A new report is displayed based on the report options that you choose.

Viewing the Traffic Statistics Details Report for a Device

The Traffic Statistics Details Report provides statistical information about the traffic transmitted on a particular WAE device. For example, you can use this report to view the total amount of traffic that a device passed-through unoptimized for the last week. Many of the statistics provided in this report are used to create the charts in the Traffic Statistics report.

To view traffic statistics details for a device, follow these steps:

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

Step 2 Click the **Edit** icon next to the device for which you want to view traffic statistics details. The Device Home window is displayed.

Step 3 From the Contents pane, choose **Acceleration > Statistics > Traffic Statistics Details**. The Application Traffic Statistics Detail Report window is displayed.

Step 4 From the Select Application drop-down list, choose the application for which you want to view statistics. By default, statistics for all applications is displayed.

Step 5 From the Time Frame drop-down list, choose one of the following options:

- **Last Hour**—Displays data for the past hour (in five-minute intervals).

- **Last Day**—Displays data for the past day (in hourly intervals).
- **Last Week**—Displays data for the past week (in daily intervals).
- **Last Month**—Displays data for the past month (in daily intervals).
- **Custom**—Displays data for the time interval you specify. After choosing this option, enter the start and ending dates for the report in the fields provided. You can also click the calendar icon next to each field to choose dates from a pop-up calendar.

Step 6 From the Direction drop-down list, choose one of the following options:

- **Outbound**—Includes traffic traveling from a client to the WAN through this WAAS device.
- **Inbound**—Includes traffic from the WAN to the client through this WAAS device
- **Bi-directional**—Includes LAN to WAN traffic as well as WAN to LAN traffic traveling through this WAAS device.

Step 7 Click **Update**.

The traffic statistics at the bottom of the window are updated based on your selections.

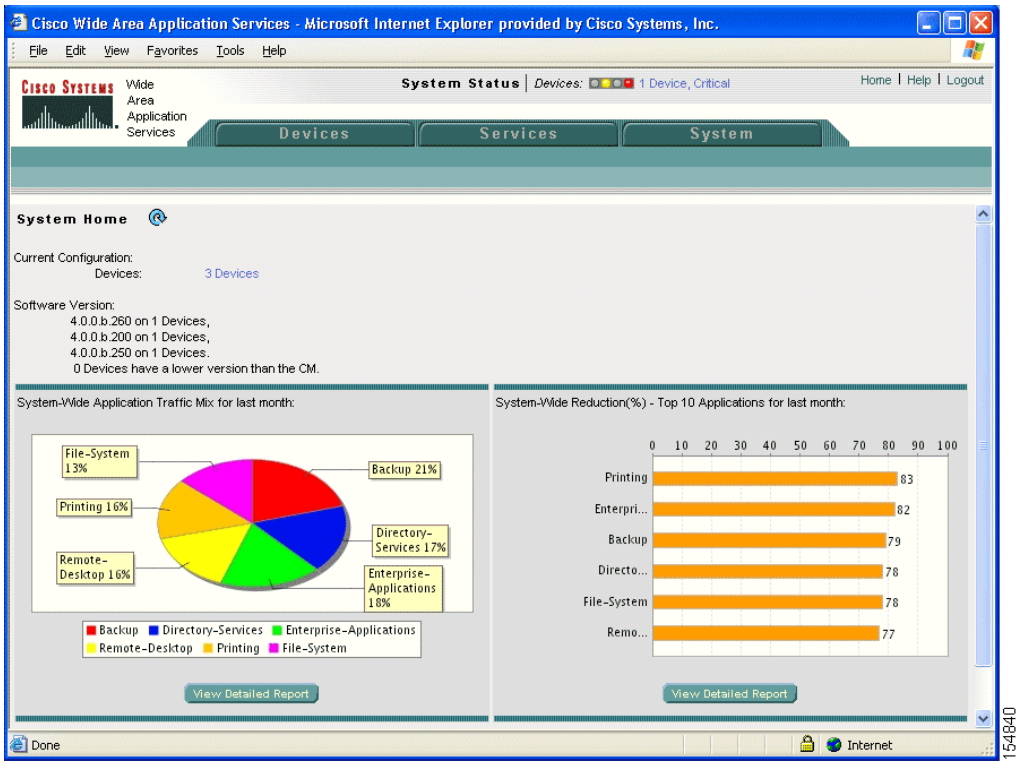
Viewing the System-Wide Traffic Statistics Report

When you first log into the WAAS Central Manager GUI, the System Home window displays the two charts that are part of the system-wide Traffic Statistics Report. These charts contain aggregated data for all the WAE devices in your WAAS network. The procedures in this section describe how to change the report options for the system-wide report.

To configure report options for the system-wide traffic statistics report, follow these steps:

Step 1 From the WAAS Central Manager GUI, click the Cisco icon in the upper left corner. The System Home window appears. (See Figure 15-11.)

Figure 15-11 System Home Window



This window displays the following information:

- Number of WAAS devices in your network
- The WAAS software versions running on your network. You can use this list to determine if any of your WAAS devices need to be upgraded to a more recent software version.

The information displayed in the System Home window is based on a snapshot of your WAAS network that represents the state of your WAE devices at the end of every two polling periods. You can configure the interval between polls in the WAAS Central Manager GUI (**System > Configuration > System Properties > System.datafeed.pollRate**). The default polling rate is 300 seconds (5 minutes).

Step 2 Click **View Detailed Report** located below either of the two displayed reports to change the report options.

The report is displayed with parameters that allow you to choose a different report and change basic properties of the report such as the time frame and size of the report.

Step 3 From the Chart drop-down list, choose one of the following chart types:

- **Reduction (incl. pass-through)**—Displays the percent of total traffic that was reduced on your entire WAAS network using the WAAS optimization techniques. This chart includes pass-through traffic in the total results.
- **Reduction (excl. pass-through)**—Displays the percent of total traffic that was reduced on your entire WAAS network using the WAAS optimization techniques. This chart excludes pass-through traffic in the total results.
- **Application Traffic Mix**—Displays the top nine applications with the most traffic for your entire WAAS network.

- **Pass-through Traffic Mix**—Displays the most common reason that traffic passed through your WAAS network unoptimized. This chart allows you to show traffic statistics for all applications or for one specific application.

For an example of each of these reports, see the "Charts in the Traffic Statistics Report" section on page 15-24.

Step 4 From the Chart Size drop-down list, choose **Small**, **Medium**, or **Large**.

Step 5 From the Time Zone drop-down list, choose one of the following options:

- **CM Local Time (default)**—Sets the time zone of the report to the time zone of the WAAS Central Manager.
- **UTC**—Sets the time zone of the report to UTC.

Note Changing the time-zone does not affect the data plotted on the graph. It only modifies the time-scale displayed to be based on the chosen time-zone.

Step 6 From the Time Frame drop-down list, choose one of the following options:

- **Last Hour**—Displays data for the past hour (in five-minute intervals).
- **Last Day**—Displays data for the past day (in hourly intervals).
- **Last Week**—Displays data for the past week (in daily intervals).
- **Last Month**—Displays data for the past month (in daily intervals).
- **Custom**—Displays data for the time interval you specify. After choosing this option, enter the start and ending dates for the report in the fields provided. You can also click the calendar icon next to each field to choose dates from a pop-up calendar.

Step 7 Choose the applications to include in the report.

If you chose one of the Reduction reports in step 3, place a check next to each application that you want to include from the list of applications displayed at the bottom of the page. To include all applications, click **All** located above the application list.

If you chose the Pass-through Traffic Mix report in step 3, use the Application drop-down list to choose the application that you want to include in the report. This drop-down list is only available for the Pass-through Traffic Mix report. To include all applications, choose **All Traffic** from the Application drop-down list.

If you chose Application Traffic Mix report in step 3, the report automatically displays the top nine applications with the most traffic. You cannot choose specific applications to include in this report.

Step 8 Click **Update**. A new report is displayed based on the report options you chose.

Charts in the Traffic Statistics Report

This section describes the following charts in the Traffic Statistics report and shows an example of each chart:

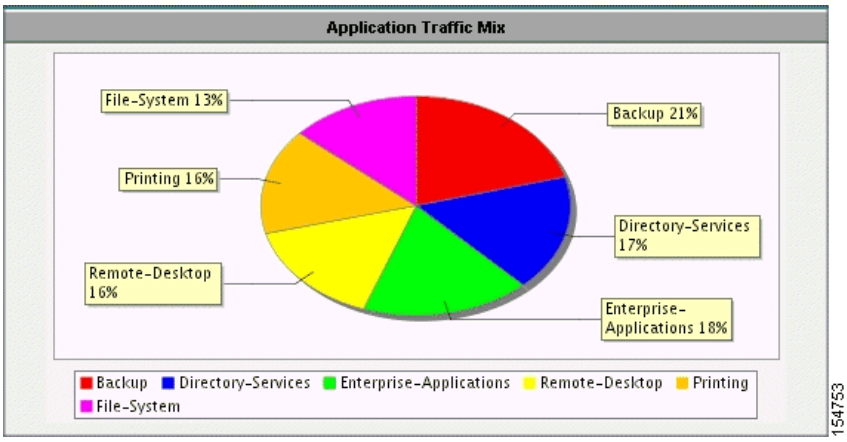
- Application Traffic Mix Chart
- Pass-through Traffic Mix Chart
- Traffic Reduction Chart

Application Traffic Mix Chart

Each section in the Application Traffic Mix chart represents an application as a percent of the total traffic on your network or device. By default, only the top nine applications with the highest percent of traffic are displayed. Nonclassified and nonmonitored applications are grouped together into the Other category.

Figure 15-12 shows an example of this chart. In this example, the Backup application is responsible for most of the traffic on the network or device.

Figure 15-12 Application Traffic Mix Chart



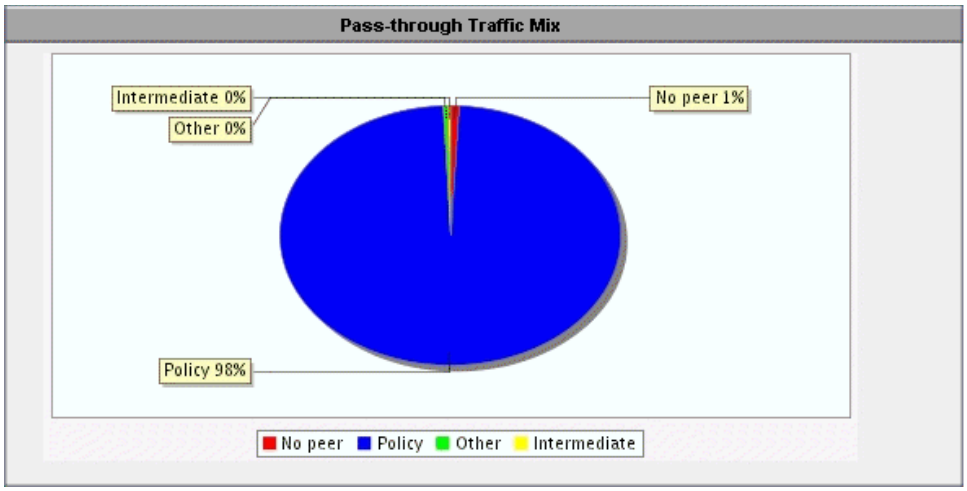
Pass-through Traffic Mix Chart

The Pass-through Traffic Mix chart shows the most common reason that traffic passed through your network or device unoptimized. WAAS devices will pass-through traffic unoptimized for the following reasons:

- **No peer**—At least two WAAS devices are required to optimize traffic over a WAN. If only one WAAS device exists along the traffic's route, then the traffic is not optimized because there is no peer WAAS device to participate in the optimization.
- **Policy**—An application policy specifies that the traffic should pass-through your network unoptimized. For information about creating and configuring application policies, see the "Creating a New Traffic Application Policy" section on page 12-2.
- **Intermediate**—When a WAE exists between two other WAEs involved in an optimized connection, traffic going through the middle WAE is passed through unoptimized.
- **Other**—Traffic that is unoptimized due to WAAS device overload, assymetric routing, blacklisting, and several other reasons.

Figure 15-13 shows an example of this chart. In this example, the most common reason that traffic is passed through unoptimized is due to the application policies that reside on the WAEs.

Figure 15-13 Pass-through Traffic Mix Chart

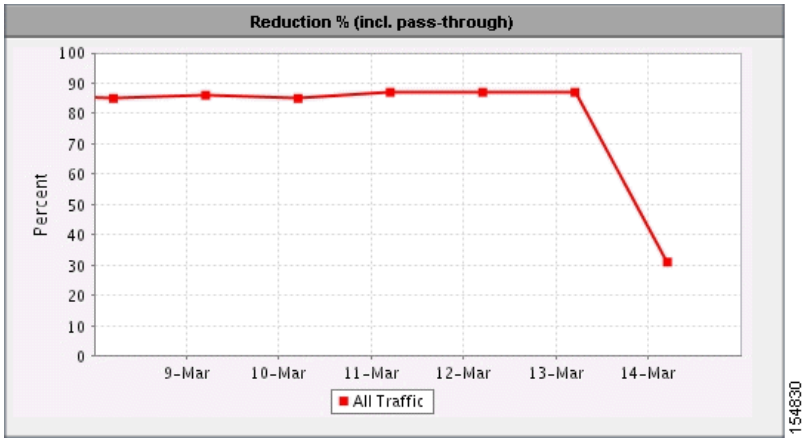


Traffic Reduction Chart

The Traffic Reduction chart shows the percent of total traffic that was reduced on your network or device using the WAAS optimization techniques. You have the option to either include pass-through traffic in this report, or to exclude pass-through traffic. If you include pass-through traffic then the total percent of reduction is less because pass-through traffic is unoptimized (not reduced).

Figure 15-14 shows an example of this chart. In this example, total network traffic was reduced by 85 percent each day over a five-day period. On the last day of the report, the total network traffic was reduced by about 30 percent.

Figure 15-14 Percent Reduction (including Pass-through Traffic) Report



Viewing CPU Utilization for a Device

To view the CPU Utilization report and configure the reporting options, follow these steps:

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

Step 2 Click the **Edit** icon next to the WAAS device for which you want to view CPU utilization.

Step 3 In the Contents pane, choose **Acceleration > Statistics > CPU Utilization**. The CPU Utilization Report window appears, displaying the statistical data. You can do the following:

- To change the report parameters and display characteristics, modify the report options as needed.
- To generate a new report based on the modified report options, click **Update**.

Enabling the Kernel Debugger

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

To enable the kernel debugger, follow these steps:

Step 1 From the WAAS Central Manager GUI, choose **Devices > Devices** (or **Devices > Device Groups**).

Step 2 Click the **Edit** icon next to the WAAS device (or device group) that you want to debug.

Step 3 Click **Show Advanced** to display the advanced menu items in the Contents pane.

Step 4 In the Contents Pane, choose **General Settings > Troubleshooting > Kernel Debugger**. The Kernel Debugger window appears.

Step 5 Check the **Enable** check box to enable the kernel debugger, and click **Submit**. By default, this option is enabled.

Troubleshooting Using the CLI

You can 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, 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 TAC.

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