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.

For additional advanced WAAS troubleshooting information, see the *Cisco WAAS Troubleshooting Guide for Release 4.1.3 and Later* on Cisco DocWiki.

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 and WAVE appliances, SM-SRE modules running WAAS, and vWAAS instances.

This chapter contains the following sections:

Viewing System Information from the System Dashboard Window

The WAAS Central Manager GUI allows you to view general and detailed information about your WAAS network from the System Dashboard window. This section describes the System Dashboard window and contains the following topics:

- Alarm Panel, page 17-3
- Device Alarms, page 17-4

Figure 17-1 shows the System Dashboard window.

Figure 17-1 System Dashboard Window

The information displayed in the charts in the System Dashboard 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 may configure the interval between polls in the WAAS Central Manager GUI (**Configure > Global > System Properties > System.monitoring.collectRate**). The default polling rate is 300 seconds (5 minutes). Alarms are presented in real time and are independent of the polling rate.

Monitoring Graphs and Charts

The default System Dashboard window contains the following graphical displays about the application traffic processed by your WAAS system:

- Traffic Summary chart—Displays the applications with the highest percentage of traffic in the WAAS network for the last hour.
- Effective WAN Capacity graph—Displays the effective increased bandwidth capacity of the WAN link as a result of WAAS optimization, as a multiple of the actual bandwidth.
- Traffic Volume and Reduction graph—Displays the original and optimized traffic volume and percentage of traffic reduction over the last hour.
- Compression Summary chart—Displays the ten applications with the highest percentage of traffic reduction for the WAAS network for the last hour. The percent calculation excludes pass-through traffic.

Numbers shown in charts and graphs are rounded to whole units (KB, MB, or GB), while those displayed in tables are rounded to three decimal places. Data values exported to CSV files are in bytes, so are not rounded.

You can customize the graphical displays and tables that are displayed on the system dashboard. For more information, see the "Customizing a Dashboard or Report" section on page 17-10. Individual charts are described in more detail in the "Chart and Table Descriptions" section on page 17-14.

Much of the device, statistical, and alarm information that is presented in the system dashboard and associated graphs and charts is also available programmatically through the monitoring API. For more information, see the *Cisco Wide Area Application Services API Reference*.

Note You must synchronize the clock on each WAE device within 5 minutes of the primary and secondary WAAS Central Managers for statistics to be consistent and reliable. For information on using an NTP server to keep all your WAAS devices synchronized, see the "Configuring NTP Settings" section on page 10-5. Additionally, if the network delay for the Central Manager to receive statistical updates from the WAEs is greater than 5 minutes, statistics aggregation may not operate as expected.

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.

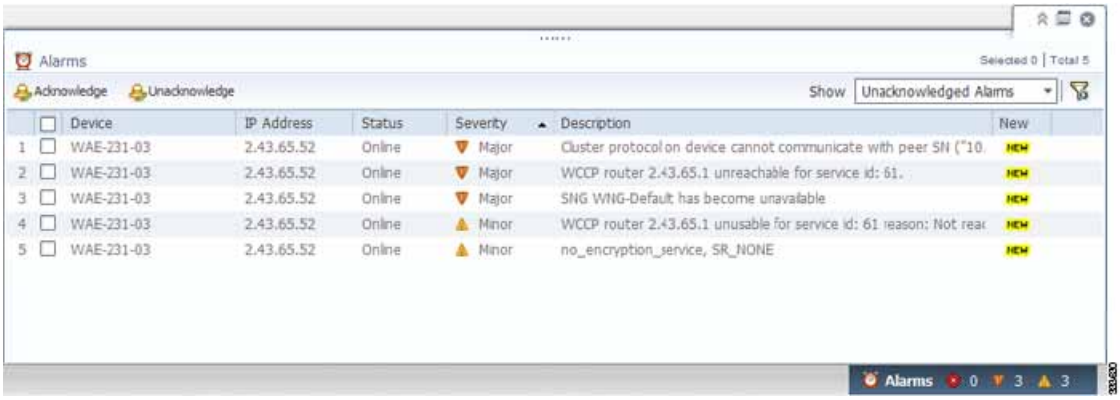
To view the alarms panel, click **Alarms** at the bottom right side of the Central Manager window.

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 17-2 shows the alarm panel.

Figure 17-2 Alarm Panel



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.

A dialog box pops up that allows you to enter comments about the alarm.

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 may use any combination of alpha, numeric, and special characters in this field.

To filter and sort 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 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 that points up for ascending order.

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 17-1 describes the various device alarms that can appear.

Table 17-1 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. This status can appear after a new device is registered but before the first configuration synchronization has been done.

Table 17-1 Device Alarms for Reporting Problems (continued)

Alarm	Alarm Severity	Device Status	Description
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

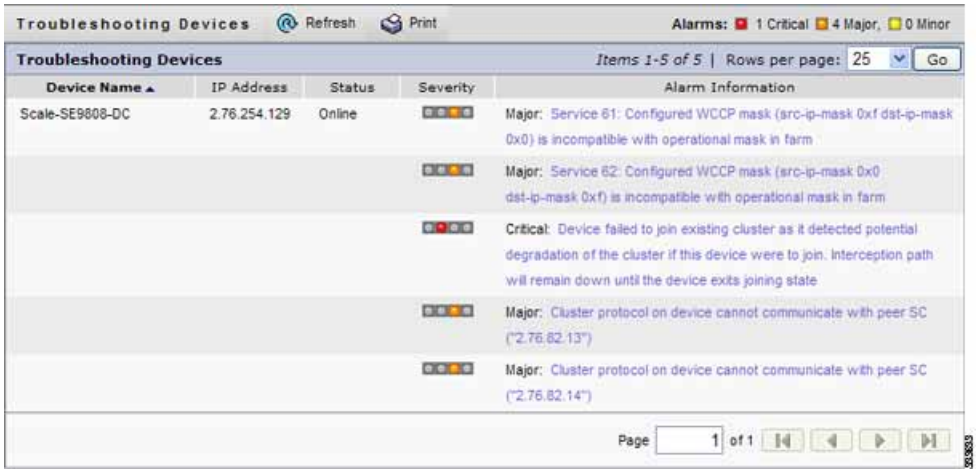
The WAAS Central Manager GUI allows you to view the alarms on each device and troubleshoot a device in the Troubleshooting Devices window.

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

Step 1 From the WAAS Central Manager menu, choose **Devices** > **All Devices** and click the device alarm light bar in the Device Status column to view alarms on a single device.

The Troubleshooting Devices window appears, either in the WAAS Central Manager window or as a separate popup window. (See Figure 17-3.)

Figure 17-3 Troubleshooting Devices Window



Step 2 In the Alarm Information column, hold your mouse over an alarm message until the Troubleshooting tools contextual menu appears. The popup menu provides links to the troubleshooting and monitoring windows in the WAAS Central Manager GUI.

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 17-2 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 17-2 Troubleshooting Tools for Device Alarms

Item	Navigation	Description
Update Software	Choose device, **Admin** > **Versioning** > **Software Update**	Displays Software Update window for this device. Appears only if the device software version is lower than the Central Manager.
Edit/Monitor Device	Device Dashboard	Displays Device Dashboard window 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 the "Using the show and clear Commands from the WAAS Central Manager GUI" section on page 17-66.

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 Dashboard 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** > **All Devices** in the WAAS Central Manager GUI.

Figure 17-4 shows an example of the Devices window.

Figure 17-4 Devices Window

This window displays the following information about each device:

- Services enabled on the device. See Table 17-3 for a description of these services.
- IP address of the device.
- Management Status (Online, Offline, Pending, or Inactive). For more information about the status, see the "Device Alarms" section on page 17-4.
- Device Status. 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 the alarm light bar, a popup message provides further details about the number of alarms. Click the alarm light bar to troubleshoot the device. For more information, see the "Troubleshooting Devices Using Alerts" section on page 17-5.
- Location associated with the device. For more information about locations, see Chapter 3, "Using Device Groups and Device Locations." You can view reports that aggregate data from all devices in a location (see the "Location Level Reports" section on page 17-36).
- Software Version installed and running on the device. For WAAS Express and AppNav-XE devices, both the Cisco IOS and the WAAS Express or AppNav-XE software versions are shown.
- Device Type. If you see a type such as OE294, the numbers refer to the model number, such as the WAVE-294 in this example. NME-WAE refers to a NME-WAE module and SM-WAE refers to a SM-SRE module. For WAAS Express and AppNav-XE devices, the router platform is displayed. For vWAAS devices, OE-VWAAS is displayed and for ISR-WAAS devices, ISR-WAAS is displayed.
- License Status. Displays the installed licenses. See Table 17-4 for a description of the possible values.

Any WAE devices that are at a higher software version level than the WAAS Central Manager are shown in red. Also, if the standby WAAS Central Manager has a different version level from the primary WAAS Central Manager, the standby WAAS Central Manager is shown in red.

You can filter your view of the devices in the list by using the Filter and Match If fields above the list. Enter a filter string in the text field and click the **Go** button to apply the filter. The filter settings are shown below the list. Click the **Clear Filter** button to clear the filter and show all devices. Filtering allows you to find devices in the list that match the criteria that you set.

Table 17-3 Service Descriptions

Service	Description
CM (Primary)	The device has been enabled as the primary WAAS Central Manager. For information on primary and standby Central Manager devices, see the "Converting a Standby Central Manager to a Primary Central Manager" section on page 16-29.
CM (Standby)	The device has been enabled as a standby WAAS Central Manager. For information on primary and standby Central Manager devices, see the "Converting a Standby Central Manager to a Primary Central Manager" section on page 16-29.
Application Accelerator	The device has been enabled as an application accelerator.
AppNav Controller	The device has been enabled as an AppNav Controller.
AppNav-XE Controller	The device is a Cisco IOS XE router with the AppNav-XE controller functionality enabled.
WAAS Express	The device is a Cisco IOS router with the WAAS Express functionality enabled.

Table 17-4 License Status Descriptions

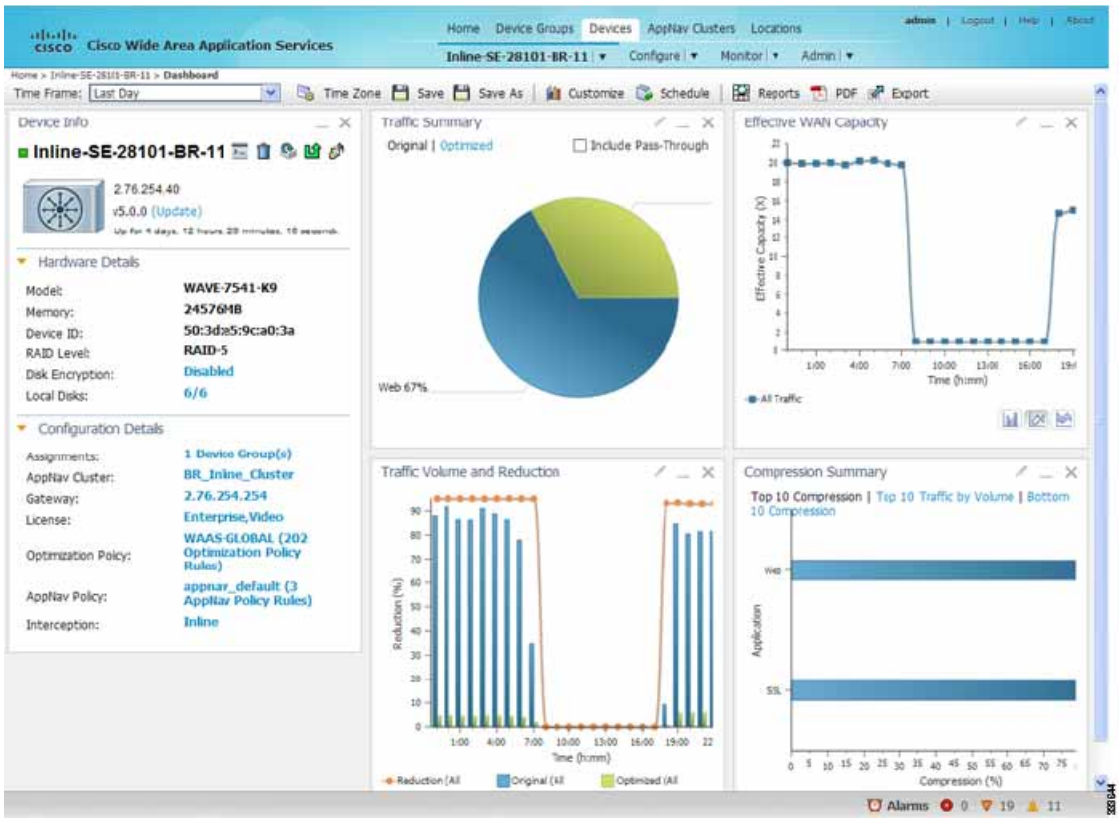
License Status	Description
Not Active	No license is installed or the first configuration synchronization has not yet happened.
Transport, Enterprise, Video, VB	The listed licenses are installed.
Active	A router device is registered but the first configuration synchronization has not yet happened.
Permanent	A router device has a permanent license installed.
Evaluation, Expires in X weeks Y days	A router device has an evaluation license installed and it expires after the indicated period.
Expired	A router device has an expired evaluation license. A permanent license must be obtained for this device to operate.
N/A	The license status is not applicable because the device version is 4.0.

Device Dashboard Window

The Device Dashboard window provides detailed information about a WAAS device such as the device model, IP address, interception method, and device-specific charts. (See Figure 17-5.)

To access the Device Dashboard window, choose **Devices** > *device-name*.

Figure 17-5 Device Dashboard Window



The Device Dashboard window for a WAAS Express or AppNav-XE device looks slightly different. It lacks some WAE-specific information and controls.

From the Device Dashboard window, you can perform the following tasks:

- View charts and graphs about the application traffic processed by the selected WAE device. (No charts or graphs are displayed if a WAAS Central Manager device is selected.)
- Customize the charts displayed in the window. For more information, see the "Customizing a Dashboard or Report" section on page 17-10. Individual charts are described in more detail in the "Chart and Table Descriptions" section on page 17-14.
- 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, the license status, and so forth.
- View the device groups to which the device belongs. For more information about device groups, see Chapter 3, "Using Device Groups and Device Locations." (Not available on AppNav-XE devices.)
- View the users that are defined on the device and unlock any locked out users. For more information, see the "Viewing and Unlocking Device Users" section on page 17-10. (Not available on WAAS Express and AppNav-XE devices.)
- Click the **Update** link to update the software on the device. For more information, see Chapter 16, "Maintaining Your WAAS System." (Not available on WAAS Express and AppNav-XE devices.)
- Click the **Telnet** icon to establish a Telnet session into the device and issue CLI commands.
- Click the **Delete Device** icon to delete the device.

- Click the **Full Update** icon to reapply the device configuration from the Central Manager to the device. (Not available on WAAS Express and AppNav-XE devices.)
- Click the **Reload** icon to reboot the device. (Not available on WAAS Express and AppNav-XE devices.)
- Click the **Restore Default Policies** icon to restore the default predefined policies on the device. For more information, see the "Restoring Optimization Policies and Class Maps" section on page 13-61. (Not available on AppNav-XE devices.)
- Assign and unassign the device to device groups. For more information, see Chapter 3, "Using Device Groups and Device Locations." (Not available on AppNav-XE devices.)
- For a WAAS Express device, a WAAS Enabled Interfaces item shows the number of interfaces on which WAAS optimization is enabled. You can click the number to go to the Network Interfaces configuration screen, which displays device interface details and allows you to enable or disable optimization on the available interfaces. For more details, see the "Configuring Optimization on WAAS Express Interfaces" section on page 6-16.
- For a WAAS Express device, you can view the DRE item to determine if the device supports data redundancy elimination (DRE) optimization, which is not supported on some WAAS Express device models. This item reads Supported or Unsupported.
- For a WAAS Express device, you can view the SSL item to determine if SSL acceleration is available. This item reads Available or Unavailable.
- For a vWAAS device, the No of CPUs, Max TCP Connections, and Interception Method fields are shown. If VPATH is enabled for the vWAAS device, it is indicated in the Interception Method field. For more details, see the "Configuring VPATH Interception on a vWAAS Device" section on page 5-56.
- On an AppNav Controller, an AppNav Cluster item shows any defined AppNav Clusters. You can click a cluster name to go to the cluster home window. Also an AppNav Policy item shows any defined AppNav policies. You can click a policy name to go to the policy configuration window.

Viewing and Unlocking Device Users

To view the users that are defined on a WAAS device, go to **Devices** > *device-name*, and then from the *device-name* menu, choose **Device Users** (on a Central Manager device, choose **CM Users**).

The list of users is displayed in a table that shows the username, number of login failures, maximum number of login failures allowed, and the time of the last failed login. To view the details on a user, click the **View** icon next to the user.

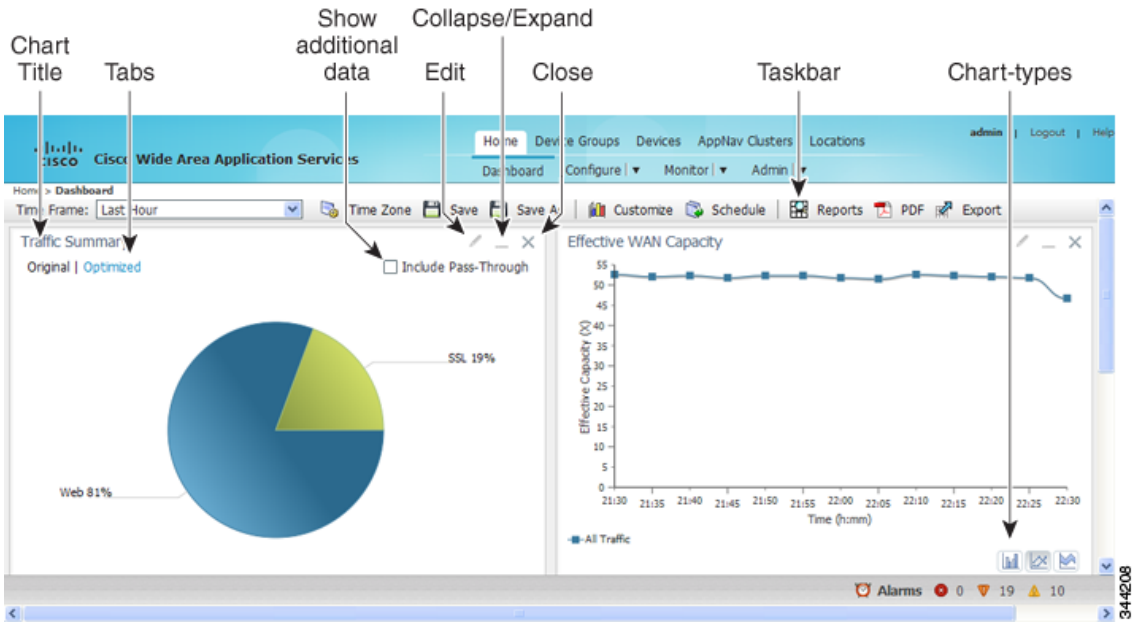
If a user is locked out because they reached the maximum number of failed login attempts, you can unlock the user by checking the box next to the username and clicking the **Unlock** button below the table.

Customizing a Dashboard or Report

You can customize the system and device dashboards and any report in the same way. For more information about creating custom reports, see the "Managing Reports" section on page 17-44.

An example of a report is shown in Figure 17-6.

Figure 17-6 Report Pane



Taskbar icons and controls across the top of the dashboard or report allow you to do the following:

- Time Frame—Allows you to choose one of the several common time frames from the drop-down list:
  - **Last Hour**—Displays data for the past hour, in five-minute intervals (default). You can change the interval using the System.monitoring.collectRate configuration setting described in the "Modifying the Default System Configuration Properties" section on page 10-17.
  - **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**—Enter starting and ending dates in the From and To fields. Click the calendar icon to choose dates from a popup calendar.

  The time frame setting is stored individually for each report and Central Manager user. Additionally, the System.monitoring.timeFrameSettings system property controls the system default time frame setting (see the "Modifying the Default System Configuration Properties" section on page 10-17).

Note If you create a chart with a custom date setting that spans more than two months back from the current date, the most recent two months of data are plotted with daily data and all previous months are plotted with aggregated monthly data. The chart might appear to have a large drop in traffic for the most recent two months because the daily traffic totals are likely to be much smaller than the monthly traffic totals; however, this difference is normal.

- Time Zone—Allows you to choose one of the following options from the Time Zone drop-down list:
  - **UTC**—Sets the time zone of the report to UTC.
  - **CM Local Time**—Sets the time zone of the report to the time zone of the WAAS Central Manager (default).

When you change the time zone, the change applies globally to all reports. The time zone setting is stored individually for each Central Manager user.

- Save—Saves the dashboard or report with its current settings. The next time you view it, it is displayed with these settings.
- Save As—Saves the report with its current settings under a new name. A popup window allows you to enter a report name and an optional description. You can enter only the following characters: numbers, letters, spaces, periods, hyphens, and underscores. The report will be available in the **Monitor > Reports > Reports Central** window.
- Customize—Allows you to add a chart or table to a dashboard or report. For information on adding a chart or table, see the "Adding a Chart or Table" section on page 17-13.
- Schedule—Allows you to schedule reports to be generated once or periodically such as hourly, daily, weekly, or monthly. When a scheduled report is generated, you can have a PDF copy of the report e-mailed to you automatically.
  - In the Date field, enter the schedule date in the format DD/MM/YYYY or click the calendar icon to display a calendar popup window from which to choose the date.
  - In the Hours drop-down list, choose the hours. The time represents the local time at the WAAS Central Manager.
  - In the Minutes drop-down list, choose the minutes. The time represents the local time at the WAAS Central Manager.
  - In the Frequency drop-down list, choose **Once**, **Hourly**, **Daily**, **Weekly**, or **Monthly** for the report frequency.
  - In the No. of Reports field, enter the number of times that a reoccurring report is to be generated. After a report is generated a specified number of times, the report is no longer generated.
  - In the Email Id(s) field, enter the e-mail addresses of the report recipients, separated by commas.
  - In the Email Subject field, enter the subject of the e-mail message.
- Reports—Allows you to view the scheduled reports. For instructions to view scheduled reports, see the "Managing Scheduled Reports" section on page 17-48.
- PDF—Generates a PDF format of the report, including the charts and table data.
- Export—Exports the chart and table statistical data to a CSV file. The statistical data shown in charts is rounded to whole units (KB, MB, or GB), while the exported data contains exact byte values.

Controls at the top of individual charts allow you to customize the chart as follows (not all controls are available in every chart):

- Chart title—Allows you to click and drag to move the chart to a different location in the report pane.
- Edit icon—Allows you to edit the chart settings as described in the "Configuring Chart Settings" section on page 17-14.
- Collapse/Expand icon—Allows you to collapse or expand the chart. When a chart is collapsed, this icon changes to Expand, which restores the chart to its normal size.
- Close icon—Closes the chart.
- Tabs—Allows you to have a choice of multiple tab views that you can access by clicking on the desired tab name (not all charts have this feature).
- Check box to show additional data—Allows you to check the box labeled with an optional data statistic to include the data in the chart (not all charts have this feature).

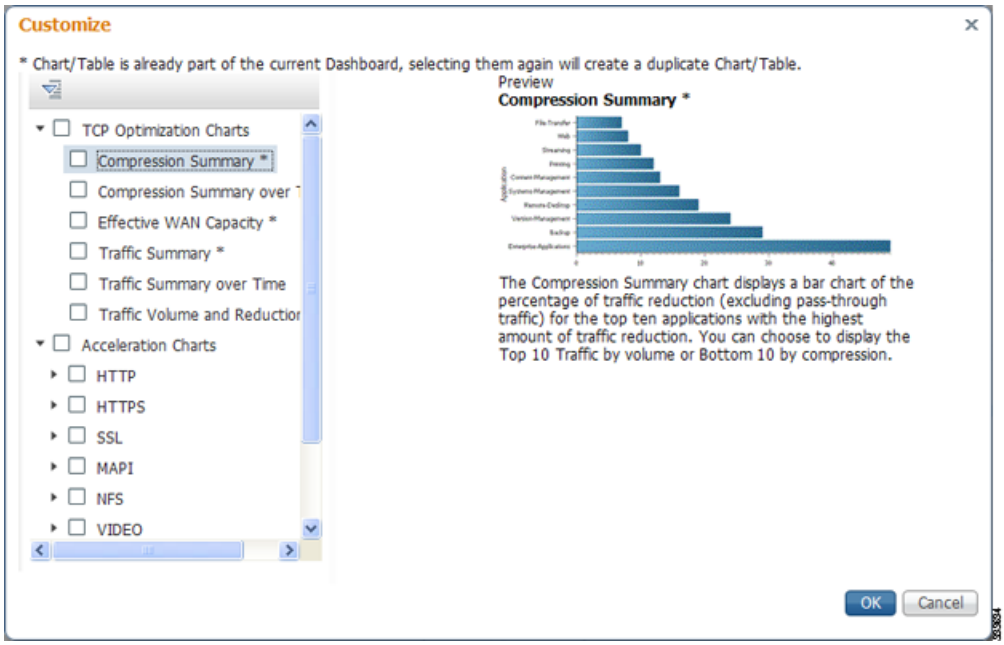
Chart-type icons at the bottom of individual charts allow you to choose the chart type as follows (not all controls are available in every chart): column chart, line chart, area chart, stacked line chart, stacked area chart.

Adding a Chart or Table

To add a chart or table to a dashboard or report, follow these steps:

Step 1 From the dashboard or report chart panel, click the **Customize** icon in the taskbar. The Customize window is displayed, as shown in Figure 17-7.

Figure 17-7 Customize Window



Step 2 Expand any of the chart categories by clicking on the small triangle next to the category.

Step 3 Check the box next to each chart or table that you want to display in the report. Individual charts are described in more detail in the "Chart and Table Descriptions" section on page 17-14.

Charts that are currently included in the dashboard or report are marked with an asterisk (*). A report can contain a maximum of eight charts and tables (the Network Summary report can contain 12).

Note At the WAAS Express device level, only charts for supported accelerators are available.

Step 4 To preview a chart, click on the chart title. The preview is displayed on the right of the pane.

Step 5 Click **OK**.

If you want to delete a chart or table from a dashboard or report, click the **Close** button on the chart and save the report.

Configuring Chart Settings

To configure the data presented in a chart, follow these steps:

Step 1 Click the **Edit** icon in the upper right corner of a chart. The Settings window is displayed.

Note Not all settings are available for all chart types.

Step 2 (Optional) From the Traffic Direction drop-down list, choose one of the following options:

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

Step 3 (Optional) In the Select Series For drop-down list, choose one of the following:

- **Application**—The chart data is based on application statistics.
- **Classifier**—The chart data is based on classifier (class map) statistics.

Step 4 (Optional) In the Application or Classifier list, check the box next to the applications or classifiers whose statistics you want to include in the chart data. To include all applications, check **All Traffic**. You can filter the list items by using the Quick Filter above the list. This list is available only for some chart types.

Step 5 (Optional) Some charts have other types of data series from which to choose. Check the box next to each data series that you want to include in the chart data.

Step 6 Click **OK**.

Note Data collection for applications and classifiers happens at slightly different times in the Central Manager, so the statistics can be different when viewing the same time period for an application and a classifier that report similar data.

Chart and Table Descriptions

This section describes the charts and tables that you can choose to include in a dashboard or report. The following categories are available:

- TCP Optimization Charts, page 17-15
- Acceleration Charts, page 17-16
- Connection Trend Charts, page 17-25
- AppNav Charts, page 17-26
- Platform Charts, page 17-28
- Statistics Details (Tables), page 17-28

All charts are plotted using the Central Manager local time zone, unless the chart settings were customized to use a different time zone.

Note At the device level for WAAS Express devices, only charts for supported accelerators are available. In all charts, pass-through traffic for WAAS Express devices is considered as zero.

TCP Optimization Charts

The following TCP optimization charts are available:

Compression Summary

The Compression Summary chart displays a bar chart of the percentage of traffic reduction (excluding pass-through traffic) for the top ten applications with the highest percentage of traffic reduction. Two additional tabs allow you to see the compression of the top ten applications by volume and the bottom ten applications with the lowest compression.

Formula:

% Reduction Excluding Pass-Through = (Original Excluding Pass-Through – Optimized) / (Original Excluding Pass-Through)

Compression Summary Over Time

The Compression Summary Over Time chart displays a graph of the percentage of total traffic that was reduced by using the WAAS optimization techniques. This chart excludes pass-through traffic in the results. You can customize the chart by choosing specific applications to include; the default is all traffic.

Formula:

% Reduction = (Original Excluding Pass-Through – Optimized) / (Original Excluding Pass-Through)

Effective WAN Capacity

The Effective WAN Capacity chart displays the effective increased bandwidth capacity of the WAN link as a result of WAAS optimization, as a value between 1X (times) and 100X. You can choose which applications to include; the default is all traffic.

Formula:

Effective WAN Capacity = 1 / (1-% Reduction Excluding Pass-Through)

% Reduction Excluding Pass-Through = (Original Excluding Pass-Through – Optimized) / (Original Excluding Pass-Through)

Throughput Summary

The Throughput Summary chart displays the amount of average and peak throughput for the LAN-to-WAN (outbound) or WAN-to-LAN (inbound) directions depending on the selected tab. The throughput units (kbps, mbps, or gbps) at the left side vary depending on the range. The Peak Throughput series is not applicable for Last Hour graphs. This chart is available only at the device and location levels. The chart in the pdf report displays a maximum of 10 series.

Formula:

% Reduction Excluding Pass-Through = (Original Excluding Pass-Through – Optimized) / (Original Excluding Pass-Through)

Traffic Summary

The Traffic Summary chart displays the top nine applications that have the highest percentage of traffic as seen by WAAS. Each section in the pie chart represents an application as a percentage of the total traffic on your network or device. Unclassified, unmonitored, and applications with less than 2 percent of the total traffic are grouped together into a tenth category named Other Traffic (shown only if it totals at least 0.1 percent of all traffic). You can choose to display Original traffic or Optimized traffic by clicking the tab, and you can include pass-through traffic by checking the Include Pass-Through check box.

Formula:

(App Traffic/ Total Traffic) * 100

App Traffic is the Original traffic (Original Excluding Pass-Through) or Optimized traffic (Optimized Excluding Pass-Through) flowing for an application.

Traffic Summary Over Time

The Traffic Summary Over Time chart displays a graph of the amount of original or optimized traffic, depending on the selected tab, and you can include pass-through traffic by checking the Pass-Through check box. You can customize the chart by choosing specific applications to include; the default is all traffic.

Traffic Volume and Reduction

The Traffic Volume and Reduction chart compares the amount of original and optimized traffic in a bar chart and displays the percentage of traffic reduction as a line. Pass-through traffic is excluded. The traffic units (bytes, KB, MB, or GB) at the right side depend upon the range. The percentage of traffic reduction is shown at the left side of the chart. You can customize the chart by choosing specific applications to include; the default is all traffic.

Formula:

% Reduction Excluding Pass-Through = (Original Excluding Pass-Through – Optimized) / (Original Excluding Pass-Through)

Acceleration Charts

This section describes these charts:

HTTP Acceleration Charts

This section describes these charts:

HTTP: Connection Details

The HTTP Connection Details chart displays the HTTP session connection statistics, showing the average number of active HTTP connections per device (at the device level for the last hour it shows the exact number). Click the **Details** tab to display the newly handled HTTP connections, optimized connections, dropped connections, and handed off connections over time.

HTTP: Effective WAN Capacity

The HTTP Effective WAN Capacity chart displays the effective bandwidth capacity of the WAN link as a result of HTTP acceleration, as a multiplier of its base capacity. The capacity data for all traffic and HTTP traffic is shown.

Note If the chart has no data, monitoring may be disabled for the application definition that includes this type of traffic. Check that monitoring is enabled for the Web application.

HTTP: Estimated Time Savings

The HTTP Estimated Time Savings chart displays a graph of the estimated percentage of the response time saved by the HTTP accelerator due to fast connection reuse, SharePoint pre-fetch optimization, and metadata caching.

HTTP: Optimization Count

The HTTP Optimization Count chart displays a graph of the number of different kinds of optimizations performed by the HTTP accelerator, which are displayed in different colors. The optimizations included in this chart are fast connection reuse, metadata caching, and SharePoint pre-fetch.

HTTP: Optimization Techniques

The HTTP Optimization Techniques pie chart displays the different kinds of optimizations performed by the HTTP accelerator. The optimizations included in this chart are fast connection reuse, metadata caching, suppressed server compression, SharePoint pre-fetch, and DRE hinting.

HTTP: Response Time Savings

The HTTP Response Time Savings chart displays a graph of the round-trip response time saved by the HTTP accelerator due to metadata caching, SharePoint pre-fetch, and fast connection reuse optimizations, which are displayed in different colors. The time units (milliseconds, seconds, or minutes) at the left side depend on the range.

HTTPS Acceleration Charts

This section describes the following charts:

HTTPS: Connection Details

The HTTPS Connection Details chart displays the HTTPS session connection statistics, showing the average number of active HTTPS connections per device (at the device level for the last hour it shows the exact number). Click the **Details** tab to display the newly handled HTTPS connections and optimized connections.

HTTPS: Effective WAN Capacity

The HTTPS Effective WAN Capacity chart displays the effective bandwidth capacity of the WAN link as a result of HTTP acceleration, as a multiplier of its base capacity. The capacity data for all traffic and SSL traffic (which includes HTTPS traffic) is shown.

Note If the chart has no data, monitoring may be disabled for the application definition that includes this type of traffic. Make sure that monitoring is enabled for the SSL application.

HTTPS: Estimated Time Savings

The HTTPS Estimated Time Savings chart displays the estimated percentage of response time saved by using metadata caching for HTTPS connections.

HTTPS: Optimization Count

The HTTPS Optimization Count chart displays a graph of the number of different kinds of metadata caching optimizations performed by the HTTPS accelerator, which are displayed in different colors.

HTTPS: Optimization Techniques

The HTTPS Optimization Techniques pie chart displays the different kinds of optimizations performed by the HTTPS accelerator. The optimizations included in this chart are metadata caching, suppressed server compression, and DRE hinting.

HTTPS: Response Time Savings

The HTTPS Response Time Savings chart displays a graph of the round-trip response time saved by the HTTPS accelerator due to metadata caching optimizations, which are displayed in different colors. The time units (milliseconds, seconds, or minutes) at the left side depend on the range.

Video Acceleration Charts

This section describes these charts:

- Video: Acceleration Bypass Reason, page 17-19
- Video: Connection Details, page 17-19
- Video: Effective WAN Capacity, page 17-19
- Video: Stream Optimization, page 17-20

Video: Acceleration Bypass Reason

The Video Acceleration Bypass Reason pie chart displays the reasons that video traffic is not accelerated: Windows Media VOD, aggregate bitrate overload, other reasons, stream bitrate overload, session count overload, and unsupported transmission type (which means an unsupported transport, unsupported player, or unsupported protocol).

Video: Connection Details

The Video Connection Details chart displays the video session connection statistics, showing the average number of active streaming video connections per device (at the device level for the last hour it shows the exact number). Click the **Details** tab to display the newly handled video connections, optimized connections, handed off connections, and dropped connections.

Video: Effective WAN Capacity

The Video Effective WAN Capacity chart displays the effective bandwidth capacity of the WAN link as a result of video acceleration, as a multiplier of its base capacity. The capacity data for all traffic and streaming video traffic is shown.

Note If the chart has no data, monitoring may be disabled for the application definition that includes this type of traffic. Check that monitoring is enabled for the Streaming application.

Video: Stream Optimization

The Video Stream Optimization chart compares the amounts of traffic incoming from the WAN and outgoing to the LAN. The traffic units (bytes, KB, MB, or GB) at the left side depend on the range.

SSL Acceleration Charts

This section describes these charts:

- SSL: Acceleration Bypass Reason, page 17-20
- SSL: Connection Details, page 17-20
- SSL: Effective WAN Capacity, page 17-20

SSL: Acceleration Bypass Reason

The SSL Acceleration Bypass Reason pie chart displays the reasons that SSL traffic is not accelerated: version mismatch, unknown, nonmatching domain, cipher mismatch, revocation failure, certificate verification failure, other failure, and non-SSL traffic.

SSL: Connection Details

The SSL Connection Details chart displays the SSL session connection statistics, showing the average number of active SSL connections per device (at the device level for the last hour it shows the exact number). Click the **Details** tab to display the newly handled SSL connections, optimized connections, handed off connections, dropped connections, HTTPS connections and ICA connections over SSL.

SSL: Effective WAN Capacity

The SSL Effective WAN Capacity chart displays the effective bandwidth capacity of the WAN link as a result of SSL acceleration, as a multiplier of its base capacity. The capacity data for all traffic and SSL traffic is shown.

Note If the chart has no data, monitoring may be disabled for the application definition that includes this type of traffic. Check that monitoring is enabled for the SSL application.

MAPI Acceleration Charts

This section describes these charts:

- MAPI: Acceleration Bypass Reason, page 17-21
- MAPI: Average Response Time Saved, page 17-21
- MAPI: Connection Details, page 17-21
- MAPI: Effective WAN Capacity, page 17-21
- MAPI: Request Optimization, page 17-21
- MAPI: Response Time Optimization, page 17-21
- MAPI: Average Accelerated Client Sessions, page 17-22

MAPI: Acceleration Bypass Reason

The MAPI Acceleration Bypass Reason pie chart displays the reasons that encrypted MAPI traffic is not accelerated: acceleration disabled, secret retriever disabled, unsupported cipher, unsupported authentication mechanism, misconfigured domain identity, failure in secret retrieval, general security failure, insufficient system resources, and recovery mode connections.

Click the **Non-Encrypted** tab to display the bypass reasons for unencrypted MAPI traffic: reservation failure (non-overload), reservation failure (overload), signed MAPI request, malformed RPC packet, handover request from peer, unsupported server version, user in denied list, unsupported client version, secured connections (encrypted), unsupported DCERPC protocol version, association group not tracked, and other.

MAPI: Average Response Time Saved

The MAPI Average Response Time Saved chart displays a graph of the estimated percentage of response time saved by the MAPI accelerator. The time units (microseconds, milliseconds, seconds, or minutes) at the left side depend upon the range.

MAPI: Connection Details

The MAPI Connection Details chart displays the MAPI session connection statistics, showing the average number of active MAPI connections per device (at the device level for the last hour it shows the exact number). Click the **Details** tab to display the newly handled MAPI connections, optimized connections, handed-off connections, and dropped connections. Click the **Optimized Encrypted vs Non-Encrypted** tab to display the new encrypted and unencrypted MAPI connections.

MAPI: Effective WAN Capacity

The MAPI Effective WAN Capacity chart displays the effective bandwidth capacity of the WAN link as a result of MAPI acceleration, as a multiplier of its base capacity. The capacity data for all traffic and MAPI traffic is shown.

Note If the chart has no data, monitoring may be disabled for the application definition that includes this type of traffic. Check that monitoring is enabled for the Email-and-Messaging application.

MAPI: Request Optimization

The MAPI Request Optimization chart displays the percentage of local and remote MAPI command responses. A local response is a response that is sent to the client from the local WAE. A remote response comes from the remote server. Click the **Encrypted vs Non-Encrypted** tab to display the percentage of local and remote responses for encrypted and unencrypted MAPI connections.

MAPI: Response Time Optimization

The MAPI Response Time Optimization chart compares the average time used for local and remote MAPI responses. The time units (microseconds, milliseconds, seconds, or minutes) at the left side depend upon the range. Click the **Encrypted vs Non-Encrypted** tab to display the average time used for local and remote responses for encrypted and unencrypted MAPI connections.

MAPI: Average Accelerated Client Sessions

The MAPI Average Accelerated Client Sessions pie chart displays the average number of encrypted sessions that are accelerated from different versions (2000, 2003, 2007, and 2010) of the Microsoft Outlook client. Click the **Non-Encrypted** tab to display the unencrypted session counts.

NFS Acceleration Charts

This section describes these charts:

NFS: Acceleration Bypass Reason

The NFS Acceleration Bypass Reason pie chart displays the reasons that NFS traffic is not accelerated: unknown authentication flavor or unknown NFS version.

NFS: Connection Details

The NFS Connection Details chart displays the NFS session connection statistics, showing the average number of active NFS connections per device (at the device level for the last hour it shows the exact number). Click the **Details** tab to display the newly handled NFS connections, optimized connections, handed-off connections, and dropped connections.

NFS: Effective WAN Capacity

The NFS Effective WAN Capacity chart displays the effective bandwidth capacity of the WAN link as a result of NFS acceleration, as a multiplier of its base capacity. The capacity data for all traffic and NFS traffic is shown.

Note If the chart has no data, monitoring may be disabled for the application definition that includes this type of traffic. Check that monitoring is enabled for the File-System application.

NFS: Estimated Time Savings

The NFS Estimated Time Savings chart displays a graph of the estimated percentage of response time saved by the NFS accelerator.

NFS: Request Optimization

The NFS Request Optimization chart displays the percentage of local and remote NFS command responses. A local response is a response that is sent to the client from the local WAE. A remote response comes from the remote server.

NFS: Response Time Optimization

The NFS Response Time Optimization chart compares the average time used for local and remote NFS responses. The time units (milliseconds, seconds, or minutes) at the left side depend upon the range.

NFS: Versions Detected

The NFS Versions Detected pie chart displays the number of NFS messages detected for each NFS version (2, 3, and 4). The NFS accelerator works with NFS version 3 traffic, so you will want to see this type of traffic for best results.

SMB Acceleration Charts

This section describes these charts:

SMB: Average Response Time Saved

The SMB Average Response Time Saved chart displays the average response time saved for SMB responses. The time units (milliseconds, seconds, or minutes) at the left side depend upon the range.

SMB: Client Average Throughput

The SMB Client Average Throughput chart displays the average client throughput for the SMB accelerator.

SMB: Connection Details

The SMB Connection Details chart displays the SMB session connection statistics, showing the average number of active SMB connections per device (at the device level for the last hour it shows the exact number). Click the **Details** tab to display the newly handled SMB connections, optimized connections, handed-off connections, dropped connections, and signed connections.

SMB: Effective WAN Capacity

The SMB Effective WAN Capacity chart displays the effective bandwidth capacity of the WAN link as a result of SMB acceleration, as a multiplier of its base capacity. The capacity data for all traffic and SMB traffic is shown.

Note If the chart has no data, monitoring may be disabled for the application definition that includes this type of traffic. Check that monitoring is enabled for the CIFS application.

SMB: Request Optimization

The SMB Request Optimization chart displays the percentage of SMB command responses that use the following optimizations: read ahead, metadata, write, and other.

SMB: Response Time Savings

The SMB Response Time Savings chart displays a graph of the round-trip response time saved by the SMB accelerator due to the following optimizations, which are displayed in different colors: read ahead, metadata, Microsoft Office, async write, named pipe, and other. The time units (milliseconds, seconds, or minutes) at the left side depend on the range.

SMB: Versions Detected

The SMB Versions Detected pie chart displays the number of SMB messages detected for each SMB version: SMB v1.0 optimized, SMB v1.0 unoptimized, SMB v1.0 signed, SMB v2.0 optimized, SMB v2.0 unoptimized, SMB v2.0 signed, SMB v2.1 optimized, SMB v2.1 unoptimized, and SMB v2.1 signed.

ICA Acceleration Charts

This section describes these charts:

- ICA: Client Versions, page 17-24
- ICA: Connection Details, page 17-24
- ICA: Effective WAN Capacity, page 17-24
- ICA: Unaccelerated Reasons, page 17-25

ICA: Client Versions

The ICA Client Versions pie chart displays the number of ICA messages detected for each ICA version: online plugin 11.0, online plugin 11.2, online plugin 12.0, online plugin 12.1, Citrix Receiver 13.0, and other.

ICA: Connection Details

The ICA Connection Details chart displays the ICA session connection statistics, showing the average number of active ICA connections per device (at the device level for the last hour it shows the exact number). Click the **Details** tab to display the newly handled ICA connections, optimized connections, handed-off connections, and dropped connections. Click the **ICA vs ICA over SSL** tab to display the the number of newly handled ICA connections and the number of newly handled ICA over SSL connections.

ICA: Effective WAN Capacity

The ICA Effective WAN Capacity chart displays the effective bandwidth capacity of the WAN link as a result of ICA acceleration, as a multiplier of its base capacity. The capacity data for all traffic and ICA traffic is shown.

Note If the chart has no data, monitoring may be disabled for the application definition that includes this type of traffic. Check that monitoring is enabled for the Citrix application.

ICA: Unaccelerated Reasons

The ICA Unaccelerated Reasons chart displays the reasons that ICA traffic is bypassed: unrecognized protocol, unsupported client version, CGP session ID unknown, client on denied list, no resource, and other. Click the **Dropped** tab to display the reasons that ICA traffic is dropped: unsupported client version, I/O error, no resource, AO parsing error, maximum sessions reached, and other.

CIFS Acceleration Charts for WAAS Express

This section describes these charts that are available only on WAAS Express devices:

- CIFS: Client Average Throughput, page 17-25
- CIFS: Connection Details, page 17-25
- CIFS: Effective WAN Capacity, page 17-25
- CIFS: Request Optimization, page 17-25

CIFS: Client Average Throughput

The CIFS Client Average Throughput chart displays the average client throughput for the WAAS Express CIFS accelerator.

CIFS: Connection Details

The CIFS Connection Details chart displays the CIFS session connection statistics for the WAAS Express CIFS accelerator, showing the average number of active CIFS connections per device (at the device level for the last hour it shows the exact number). Click the **Details** tab to display the newly handled CIFS connections, optimized connections, handed-off connections, and dropped connections.

CIFS: Effective WAN Capacity

The CIFS Effective WAN Capacity chart displays the effective bandwidth capacity of the WAN link as a result of WAAS Express CIFS acceleration, as a multiplier of its base capacity. The capacity data for all traffic and CIFS traffic is shown.

CIFS: Request Optimization

The CIFS Request Optimization chart displays the percentage of WAAS Express CIFS accelerator command responses that use the following optimizations: read ahead, metadata, write, and other.

Connection Trend Charts

This section describes these charts:

- Optimized Connections Over Time, page 17-26
- Optimized vs Pass-Through Connections, page 17-26

Optimized Connections Over Time

The Optimized Connections Over Time chart displays the number of optimized connections over the selected time period. You can show the number of MAPI reserved connections by checking the **MAPI Reserved Connections** check box. You can view the peak optimized connection values for all the data points in the chart by checking the **Peak Connections** check box. For WAAS-EX devices, Optimized Connections Over Time chart has only the Peak Connections option. You can customize the chart by choosing specific applications to include; the default is all traffic.
This chart is available only when a specific WAAS device is selected and can be added only to the Connection Trend report.

Optimized vs Pass-Through Connections

The Optimized vs Pass-Through Connections chart displays the total number of optimized and pass-through connections on a device or on all devices in a location. You can show the device connection limit, which is the maximum number of connections a device can support, by checking the **Device Connection Limit** check box. This option is available only at the device level. At the Location level, by default the chart displays only the top five devices series based on the maximum connection limit usage. You can select the devices of your choice from the chart **Settings** page. The chart in the pdf report displays a maximum of 10 series.
You can view the peak pass- through connection values for all the data points in the chart by checking the **Peak Connections** check box.

This chart is available only when a specific WAAS device or location is selected and can be added only to the Connection Trend report.

Formula:

Pass-Through Connections for a Device = Total Pass-Through Connections for all applications

Optimized Connections for a Device = Total Optimized Connections for all applications

Device Connections limit usage % = 100 * Average Optimized connections/ Device connection Limit

where,

Average Optimized connections = Sum of Optimized Connections / no. of samples

AppNav Charts

This section describes these charts:

- Total AppNav Traffic, page 17-27
- AppNav Policies, page 17-27
- Top 10 AppNav Policies, page 17-27
- Top 10 WAAS Node Group Distribution, page 17-27
- WAAS Node Group Distribution, page 17-27
- Pass-Through Reasons, page 17-27
- Top 10 Pass-Through Reasons, page 17-27

Total AppNav Traffic

The Total AppNav Traffic chart displays the total amount of distributed and pass-through traffic processed by the AppNav Cluster or ANC device. The units at the left side depend upon the range.

AppNav Policies

The AppNav Policies chart displays a graph of the amount of intercepted, distributed, or pass-through traffic processed by the AppNav Cluster or ANC device for each policy rule, depending on which tab you select. The units at the left side depend upon the range.

From the Show Details For drop-down list, you can select a policy rule for which to show details.

Top 10 AppNav Policies

The Top 10 AppNav Policies pie chart displays the amount of intercepted, distributed, or pass-through traffic processed by the AppNav Cluster or ANC device for the top nine policy rules with the most traffic, depending on which tab you select. Traffic for all other policy rules is grouped together into a tenth category named Other Traffic (shown only if it totals at least 0.1 percent of all traffic).

From the Show Details For drop-down list, you can select a policy rule for which to show details.

Top 10 WAAS Node Group Distribution

The Top 10 WAAS Node Group Distribution pie chart displays the top nine WNGs to which traffic is distributed. Traffic for all other WNGs is grouped together into a tenth category named Other Traffic (shown only if it totals at least 0.1 percent of all traffic).

From the Show Details For drop-down list, you can select a WNG for which to show details of the individual WNs.

WAAS Node Group Distribution

The WAAS Node Group Distribution chart displays a graph of the amount of traffic distributed to each of the WAAS node groups (WNGs). The units at the left side depend upon the range.

From the Show Details For drop-down list, you can select a WNG for which to show details of the individual WAAS nodes (WNs).

Pass-Through Reasons

The Pass-Through Reasons chart displays a graph of the amount of pass-through traffic for each of the pass-through reasons. The units at the left side depend upon the range.

From the Show Details For drop-down list, you can select a reason for which to show details.

Top 10 Pass-Through Reasons

The Top 10 Pass-Through Reasons pie chart displays the top nine reasons that traffic is passed through. Traffic for all other reasons is grouped together into a tenth category named Other Traffic (shown only if it totals at least 0.1 percent of all traffic).

From the Show Details For drop-down list, you can select a reason for which to show details.

Platform Charts

This section describes these charts:

CPU Utilization

The CPU Utilization chart displays the percentage of CPU utilization for the device. This chart is available only when a specific WAAS device is selected. This chart can be added only to the **Monitor** > **Reports** > **Reports Central** > **Resource Utilization** report page.

Disk Utilization

The Disk Utilization chart displays the percentage of disk utilization for the device. This chart is available only when a specific WAAS device is selected. This chart can be added only to the **Monitor** > **Reports** > **Reports Central** > **Resource Utilization** report page.

Statistics Details (Tables)

The following statistics details tables are available:

You can sort the tables by clicking on any column heading to sort on data in that column. A small triangle control appears in the heading to indicate that the table is sorted on this column. Click the triangle to reverse the sort order for the column.

For some values, different formulas are used at the system and device levels, and these formulas are noted in the table descriptions. The terms used in the tables are defined as follows:

- Original Inbound—Traffic that is entering the WAAS device from the LAN (clients) and needs to be optimized before being sent out on the WAN to a peer WAAS device.
- Original Outbound—Traffic that is exiting the WAAS device to the LAN (clients) after being received on the WAN from a peer WAAS device.
- Optimized Inbound—Traffic that is entering the WAAS device from the WAN and needs to be processed (deoptimized) before being sent out on the LAN to clients.

- Optimized Outbound—Traffic that is exiting the WAAS device to the WAN and a peer WAAS device after being optimized.
- Pass-Through—Traffic that is being passed through the WAAS device and not optimized.

To get the statistics at the system, location, and device group levels, the Original Inbound, Original Outbound, Optimized Inbound, Optimized Outbound, Pass-through Client, and Pass-through Server bytes of all devices are added together. The Reduction % and Effective Capacity values are calculated using these added values of all devices.

Traffic Summary Table

This table is called the Network Traffic Summary, Device Traffic Summary, or Location Traffic Summary, depending on the context and it displays a summary of traffic.

At the system and location levels, each row in the table displays the total traffic information for each device that is registered to this Central Manager or is in this location. At the device level, each row in the table displays the total traffic information for each application defined on the device. The data is described in Table 17-5.

Table 17-5 Traffic Summary Table

Table Column	Description and Formulas Used to Calculate Value
Device	The device name. (Appears only at the system and location levels.)
Application	The application name. (Appears only at the device level. At the system level, use the Network Application Traffic Details Table to get this information.)
Original Traffic (Excludes Pass-Through)	Reports the amount of original traffic, excluding pass-through traffic. System: (Original Outbound + Original Inbound)/2 Device/Device Group: Original Inbound + Original Outbound
Optimized Traffic (Excludes Pass-Through)	Reports the amount of optimized traffic, excluding pass-through traffic. System: (Optimized Inbound + Optimized Outbound)/2 Device/Device Group: Optimized Outbound + Optimized Inbound
Pass-Through Traffic	Reports the amount of pass-through traffic. This value is not applicable for WAAS Express devices. System: (Pass-through Client + Pass-through Server)/2 Device/Device Group: Pass-through Client + Pass-through Server An asterisk (*) in the column heading indicates that a device whose data is included in this table is configured as a serial peer with another device and optimization is disabled between those two peer devices. The amount of pass-through traffic shown may be more than what is expected because the device passes through traffic coming from its peer (for more information, see the "Information About Clustering Inline WAEs" section on page 5-53).[1]

Table 17-5 Traffic Summary Table

Table Column	Description and Formulas Used to Calculate Value
Reduction (%)	Reports the percentage of bytes saved, considering only optimized traffic. (Original Excl Pass-through – (Optimized)) * 100 / (Original Excl Pass-through)
Effective Capacity	Reports the effective bandwidth capacity of the WAN link as a result of optimization, as a multiplier of its base capacity, considering only optimized traffic. 1/(1 – % Reduction Excl Pass-through)

1. The number in the Pass-Through Traffic column represents the amount of traffic that is passed through that particular WAE (or for a location report, all the devices in the location). If the device is part of a serial inline cluster (that is, configured as a non-optimizing peer with another device), the traffic that is shown as pass-through on one device may have been optimized by another device in the serial cluster. It is useful to know the amount of traffic that is not optimized by either of the devices in the cluster (in other words, passed through the entire cluster).

   When the device closer to the LAN is not overloaded, the pass through numbers on that device accurately represent the overall pass-through traffic. But, if that device goes into overload, the second device in the cluster starts optimizing traffic that was passed through by the first one, which needs to be accounted for. In this case, the overall pass-through numbers for the cluster can be obtained as follows. Note that this calculation has to be done even if the first device went into overload in the past and came out of it.

   Consider that W1 and W2 are part of a serial cluster and W1 is toward the LAN (closer to the client if the cluster is in the branch, or closer to the server if the cluster is in the data center) and W2 is toward the WAN. The amount of traffic that is passed through the cluster without optimization by either W1 or W2 can be obtained by the following formula: (W1 pass-through traffic) – (W2 original traffic)

Network Application Traffic Details Table

The Network Application Traffic Details table is available at the system level and displays the total traffic information for each application. The data is the same as described in Table 17-5 (except there is no Device column in this table).

HTTP Acceleration Statistics Table

The HTTP Acceleration Statistics table is available at the system and device levels and displays HTTP acceleration details. The data is described in Table 17-6.

Table 17-6 HTTP Acceleration Statistics Table

Table Column	Description and Formulas Used to Calculate Value
Device	The device name. (Appears only at the system level.)
Start Time and End Time	Start and end times for the time period. (Appears only at the device level.)
New Connections Handled	Reports the number of HTTP connections handled for the time period.
Average Active Connections/ Active Connections	Reports the average active number of connections currently being handled by the HTTP accelerator at the system level. At other levels, reports the number of active connections.
New Bypassed Connections	Reports the number of connections initially received by the HTTP accelerator and then pushed down to the generic accelerator.
Total Time Saved	Reports the amount of time saved due to HTTP optimization.

Table 17-6 HTTP Acceleration Statistics Table

Table Column	Description and Formulas Used to Calculate Value
Total Round-Trip Time	Reports the total round-trip time for all connections plus the time for remotely served metadata cache misses.
% Time Saved	Reports the percentage of connection time saved for all aggregated samples. Total Time Saved / (Total Time Saved + Total Round Trip Time For All Connections + Total time for all remotely served metadata cache misses)

HTTPS Acceleration Statistics Table

The HTTPS Acceleration Statistics table is available at the system and device levels and displays HTTPS acceleration details. The data is described in Table 17-7.

Table 17-7 HTTPS Acceleration Statistics Table

Table Column	Description and Formulas Used to Calculate Value
Device	The device name. (Appears only at the system level.)
Start Time and End Time	Start and end times for the time period. (Appears only at the device level.)
New Connections Handled	Reports the number of HTTPS connections handled for the time period.
Average Active Connections/ Active Connections	Reports the average number of connections currently being handled by the HTTP/SSL accelerator at the system level. At other levels, reports the number of active connections.
Total Time Saved	Reports the amount of time saved due to HTTPS optimization.
Total Round-Trip Time	Reports the total round-trip time for all connections plus the time for remotely served metadata cache misses.
% Time Saved	Reports the percentage of connection time saved for all aggregated samples. Total Time Saved by cache hits / (Total Time Saved by cache hits + Total time for all remotely served metadata cache misses)

ICA Acceleration Statistics Table

The ICA Acceleration Statistics table is available at the system and device levels and displays ICA acceleration details. The data is described in Table 17-8.

Table 17-8 ICA Acceleration Statistics Table

Table Column	Description and Formulas Used to Calculate Value
Device	The device name. (Appears only at the system level. WAAS Express devices are not included.)
Start Time and End Time	Start and end times for the time period. (Appears only at the device level.)
New Connections Handled	Reports the number of ICA connections handled for the time period.
Average Active Connections/ Active Connections	Reports the average number of connections currently being handled by the ICA accelerator at the system level. At other levels, reports the number of active connections.

Table 17-8 ICA Acceleration Statistics Table

Table Column	Description and Formulas Used to Calculate Value
Dropped Connections	Reports the number of connections dropped by the ICA accelerator.
Bypassed Connections	Reports the number of connections initially received by the ICA accelerator and then pushed down to the generic accelerator.

MAPI Acceleration Statistics Table

The MAPI Acceleration Statistics table is available at the system and device levels and displays MAPI acceleration details. The data is described in Table 17-9.

Table 17-9 MAPI Acceleration Statistics Table

Table Column	Description and Formulas Used to Calculate Value
Device	The device name. (Appears only at the system level. WAAS Express devices are not included.)
Start Time and End Time	Start and end times for the time period. (Appears only at the device level.)
New Connections Handled	Reports the number of MAPI connections handled for the time period.
Average Active Connections/ Active Connections	Reports the average number of connections currently being handled by the MAPI accelerator at the system level. At other levels, reports the number of active connections.
New Bypassed Connections	Reports the number of connections initially received by the MAPI accelerator and then pushed down to the generic accelerator.
New Local Request Count	Reports the number of client requests handled locally by the WAE.
Avg. Local Response Time	Reports the average time used for local responses, in microseconds.
New Remote Request Count	Reports the number of client requests handled remotely over the WAN.
Avg. Remote Response Time	Reports the average time used for remote responses, in microseconds.
Average Time Saved	Reports the average connection time saved for all aggregated samples, in microseconds.

NFS Acceleration Statistics Table

The NFS Acceleration Statistics table is available at the system and device levels and displays NFS acceleration details. The data is described in Table 17-10.

Table 17-10 NFS Acceleration Statistics Table

Table Column	Description and Formulas Used to Calculate Value
Device	The device name. (Appears only at the system level. WAAS Express devices are not included.)
Start Time and End Time	Start and end times for the time period. (Appears only at the device level.)
New Connections Handled	Reports the number of NFS connections handled for the time period.
Average Active Connections/ Active Connections	Reports the average number of connections currently being handled by the NFS accelerator at the system level. At other levels, reports the number of active connections.

Table 17-10 NFS Acceleration Statistics Table

Table Column	Description and Formulas Used to Calculate Value
New Bypassed Connections	Reports the number of connections initially received by the NFS accelerator and then pushed down to the generic accelerator.
New Local Request Count	Reports the number of client requests handled locally by the WAE.
Avg. Local Response Time	Reports the average time used for local responses, in milliseconds.
New Remote Request Count	Reports the number of client requests handled remotely over the WAN.
Avg. Remote Response Time	Reports the average time used for remote responses, in milliseconds.
% Time Saved	Reports the percentage of connection time saved for all aggregated samples. (Down – Up) * 100 / (Down) If(Down != 0) where: Down = (New local request count + New remote request count) * Avg. local response time Up = ((New local request count * Avg. local response time) + (New remote request count * Avg. remote response time))

SMB Acceleration Statistics Table

The SMB Acceleration Statistics table is available at the system and device levels and displays SMB acceleration details. The data is described in Table 17-11.

Table 17-11 SMB Acceleration Statistics Table

Table Column	Description and Formulas Used to Calculate Value
Device	The device name. (Appears only at the system level. WAAS Express devices are not included.)
Start Time and End Time	Start and end times for the time period. (Appears only at the device level.)
New Connections Handled	Reports the number of SMB connections handled for the time period.
Average Active Connections/ Active Connections	Reports the average number of connections currently being handled by the SMB accelerator at the system level. At other levels, reports the number of active connections.
Bypassed Connections	Reports the number of connections initially received by the SMB accelerator and then pushed down to the generic accelerator.
Total Time Saved	Reports the amount of time saved due to SMB optimization.
Total Round-Trip Time	Reports the total round-trip time for all connections plus the time for remotely served metadata cache misses.
% Time Saved	Reports the percentage of connection time saved for all aggregated samples. Total Time Saved by cache hits / (Total Time Saved by cache hits + Total Time for all remotely served metadata cache misses)

SSL Acceleration Statistics Table

The SSL Acceleration Statistics table is available at the system and device levels and displays SSL acceleration details. The data is described in Table 17-12.

Table 17-12 SSL Acceleration Statistics Table

Table Column	Description
Device	The device name. (Appears only at the system level.)
Start Time and End Time	Start and end times for the time period. (Appears only at the device level.)
New Connections Handled	Reports the number of SSL connections handled for the time period.
Average Active Connections/ Active Connections	Reports the average number of connections currently being handled by the SSL accelerator at the system level. At other levels, reports the number of active connections.
New HTTPS Connections Handled	Reports the number of HTTPS connections handled by the SSL accelerator.
Dropped Connections	Reports the number of connections dropped by the SSL accelerator.
Bypassed Connections	Reports the number of connections initially received by the SSL accelerator and then pushed down to the generic accelerator.

Video Acceleration Statistics Table

The Video Acceleration Statistics table is available at the system and device levels and displays video acceleration details. The data is described in Table 17-13.

Table 17-13 Video Acceleration Statistics Table

Table Column	Description
Device	The device name. (Appears only at the system level.)
Start Time and End Time	Start and end times for the time period. (Appears only at the device level.)
New Connections Handled	Reports the number of video connections handled for the time period.
Average Active Connections/ Active Connections	Reports the average number of connections currently being handled by the video accelerator at the system level. At other levels, reports the number of active connections.
New Bypassed Connections	Reports the number of connections initially received by the video accelerator and then pushed down to the generic accelerator.

CIFS Acceleration Statistics Table for WAAS Express

The CIFS Acceleration Statistics table displays CIFS acceleration details for a WAAS Express device. The data is described in Table 17-14.

Table 17-14 CIFS Acceleration Statistics Table

Table Column	Description and Formulas Used to Calculate Value
Start Time and End Time	Start and end times for the time period. (Appears only at the device level.)
New Connections Handled	Reports the number of CIFS connections handled for the time period.

Table 17-14 CIFS Acceleration Statistics Table

Table Column	Description and Formulas Used to Calculate Value
Average Active Connections/ Active Connections	Reports the average number of connections currently being handled by the CIFS accelerator at the system level. At other levels, reports the number of active connections.
Bypassed Connections	Reports the number of connections initially received by the CIFS accelerator and then pushed down to the generic accelerator.
Total Time Saved	Reports the amount of time saved due to CIFS optimization.
Total Round-Trip Time	Reports the total round-trip time for all connections plus the time for remotely served metadata cache misses.
% Time Saved	Reports the percentage of connection time saved for all aggregated samples. Total Time Saved by cache hits / (Total Time Saved by cache hits + Total time for all remotely served metadata cache misses)

Using Predefined Reports to Monitor WAAS

The WAAS Central Manager includes a number of predefined reports that you can use to monitor the system operation. These reports are available in the Monitor menu. The reports consist of a combination of specific charts and graphs and a statistical table displayed in the lower part of the window.

You can customize these predefined reports by editing them with the Manage Report function available in the Monitor menu, as described in the "Viewing and Editing Reports" section on page 17-46.

The following predefined reports are available at the WAAS system level, the AppNav Cluster level, the location level, and the device level:

- Optimization
  - TCP Summary Report, page 17-36
- Acceleration (not all are available at the WAAS Express device level)
  - HTTP Acceleration Report, page 17-37
  - HTTPS Acceleration Report, page 17-37
  - Video Acceleration Report, page 17-37
  - SSL Acceleration Report, page 17-38
  - MAPI Acceleration Report, page 17-38
  - NFS Acceleration Report, page 17-38
  - SMB Acceleration Report, page 17-38
  - ICA Acceleration Report, page 17-39

The following predefined report is available only at the WAAS System level:

- Network > Summary Report, page 17-39

The following predefined report is available only at the WAAS System level and the device level:

- Network/Peers > Topology Report, page 17-40

The following predefined report is available only at the device level and the location level:

- Optimization > Connection Trend Report, page 17-40

The following predefined reports are available only at the device level:

- Optimization
  - Connections Statistics Report, page 17-40
- Acceleration
  - CIFS Acceleration Report, page 17-42 (not available for a WAAS Express device)
  - CIFS Acceleration Report for WAAS Express, page 17-42 (available only for a WAAS Express device)
- Platform (not available at the WAAS Express or AppNav-XE device level)
  - Resource Utilization Report, page 17-42
  - Disks Report, page 17-43

The following predefined reports are available only at the AppNav Cluster level and at the device level for AppNav Controller devices:

- AppNav > AppNav Report, page 17-43

Note In a WAAS network where there are 1000 or more WAEs, there may be a delay of up to 90 seconds to redisplay the table when you click a table column to resort any system level report table. You may experience a similar delay when you click the Print icon in the taskbar, before you see the report.

Location Level Reports

Location level reports aggregate data from all the WAEs present in a particular location. For more information about locations, see the "Working with Device Locations" section on page 3-10.

To view a location level report, follow these steps:

Step 1 From the WAAS Central Manager menu, choose **Locations** > *location-name*.

Step 2 Choose **Monitor** and choose the report from the Optimization or Acceleration categories.

When scheduling any report, you can also select one or more locations and the report will include data from all devices within the selected locations. For more information, see the "Scheduling Reports" section on page 17-46.

The maximum number of devices supported in a location level report is 25 by default. This number is configurable up to 250 by the System.monitoring.maxDevicePerLocation system property. For more information, see the "Modifying the Default System Configuration Properties" section on page 10-17.

TCP Summary Report

The TCP Summary report displays a summary of all traffic. The following charts and tables are included:

- Traffic Summary, page 17-16
- Effective WAN Capacity, page 17-15
- Traffic Volume and Reduction, page 17-16

- Compression Summary, page 17-15
- Traffic Summary Over Time, page 17-16
- Compression Summary Over Time, page 17-15
- Throughput Summary, page 17-16 (included only at the device and location levels)
- Traffic Summary Table, page 17-29

HTTP Acceleration Report

The HTTP Acceleration report displays the HTTP acceleration statistics. The following charts and tables are included:

- HTTP: Estimated Time Savings, page 17-17
- HTTP: Effective WAN Capacity, page 17-17
- HTTP: Connection Details, page 17-17
- HTTP: Response Time Savings, page 17-18
- HTTP: Optimization Count, page 17-18
- HTTP: Optimization Techniques, page 17-18
- HTTP Acceleration Statistics Table, page 17-30

HTTPS Acceleration Report

The HTTPS Acceleration report displays the HTTPS acceleration statistics. The following charts and tables are included:

- HTTPS: Estimated Time Savings, page 17-18
- HTTPS: Effective WAN Capacity, page 17-18
- HTTPS: Connection Details, page 17-18
- HTTPS: Response Time Savings, page 17-19
- HTTPS: Optimization Count, page 17-19
- HTTPS: Optimization Techniques, page 17-19
- HTTPS Acceleration Statistics Table, page 17-31

Video Acceleration Report

The Video Acceleration report displays the video acceleration statistics. The following charts and tables are included:

- Video: Stream Optimization, page 17-20
- Video: Effective WAN Capacity, page 17-19
- Video: Connection Details, page 17-19
- Video: Acceleration Bypass Reason, page 17-19
- Video Acceleration Statistics Table, page 17-34

SSL Acceleration Report

The SSL Acceleration report displays the SSL acceleration statistics. The following charts and tables are included:

- SSL: Connection Details, page 17-20
- SSL: Effective WAN Capacity, page 17-20
- SSL: Acceleration Bypass Reason, page 17-20
- SSL Acceleration Statistics Table, page 17-34

MAPI Acceleration Report

The MAPI Acceleration report displays the MAPI acceleration statistics. The following charts and tables are included:

- MAPI: Average Response Time Saved, page 17-21
- MAPI: Effective WAN Capacity, page 17-21
- MAPI: Connection Details, page 17-21
- MAPI: Request Optimization, page 17-21
- MAPI: Response Time Optimization, page 17-21
- MAPI: Average Accelerated Client Sessions, page 17-22
- MAPI: Acceleration Bypass Reason, page 17-21
- MAPI Acceleration Statistics Table, page 17-32

NFS Acceleration Report

The NFS Acceleration report displays the NFS acceleration statistics. The following charts and tables are included:

- NFS: Estimated Time Savings, page 17-22
- NFS: Effective WAN Capacity, page 17-22
- NFS: Connection Details, page 17-22
- NFS: Request Optimization, page 17-22
- NFS: Response Time Optimization, page 17-23
- NFS: Versions Detected, page 17-23
- NFS: Acceleration Bypass Reason, page 17-22
- NFS Acceleration Statistics Table, page 17-32

SMB Acceleration Report

The SMB Acceleration report displays the SMB acceleration statistics. The following charts and tables are included:

- SMB: Average Response Time Saved, page 17-23

- SMB: Effective WAN Capacity, page 17-23
- SMB: Connection Details, page 17-23
- SMB: Request Optimization, page 17-24
- SMB: Response Time Savings, page 17-24
- SMB: Client Average Throughput, page 17-23
- SMB: Versions Detected, page 17-24
- SMB Acceleration Statistics Table, page 17-33

ICA Acceleration Report

The ICA Acceleration report displays the ICA acceleration statistics. The following charts and tables are included:

- ICA: Effective WAN Capacity, page 17-24
- ICA: Connection Details, page 17-24
- ICA: Client Versions, page 17-24
- ICA: Unaccelerated Reasons, page 17-25
- ICA Acceleration Statistics Table, page 17-31

Note The ICA charts in WAAS version 5.0 and later are different from those used in version 4.5. If you are viewing the data from a version 4.5 WAAS device, the charts appear empty due to the different data that the device is collecting. The ICA data for version 4.5 WAAS devices is available in the system level TCP Summary Report.

Summary Report

The Summary Report is a predefined report that can be used to monitor the system operation. It is available at the system level. This report displays the following charts and tables by default:

- Traffic Summary, page 17-16
- Effective WAN Capacity, page 17-15
- Traffic Summary Over Time, page 17-16
- Traffic Volume and Reduction, page 17-16
- Compression Summary, page 17-15
- Compression Summary Over Time, page 17-15
- HTTP: Estimated Time Savings, page 17-17
- HTTP: Effective WAN Capacity, page 17-17
- MAPI: Effective WAN Capacity, page 17-21
- SSL: Effective WAN Capacity, page 17-20
- MAPI: Average Response Time Saved, page 17-21
- Network Application Traffic Details Table, page 17-30

The Summary Report can be customized to display the charts that you require. Use the Customize taskbar icon to select the charts that you want to be displayed on this report. Only 12 charts can be displayed in the report.

Topology Report

The Topology report at the system level displays a topology map that shows a graphical representation of all the connections between the WAAS devices.

The topology map uses blue squares to show connections between devices. Use the legend to the right of the grid to associate the device name with the number that appears at the top of the grid. Use the drop-down lists at the top of the window to perform the following tasks:

- Display connections between your various locations instead of between devices.
- Sort the grid by the number of connections instead of by device name.

Click the **View** icon next to the WAE to view a list of peer devices for a specific WAE. The Peer List window appears, which is the same as the device level Topology report.

At the device level, the Topology report lists all the peer devices connected to a specific WAE so that you can see the relationship between devices in your WAAS network. The Peer List window displays information about each peer device involved in optimized connections with this WAE. To go to the system level Topology report, click the **Topology** icon in the taskbar.

If a peer device is not registered with the WAAS Central Manager, the message “Unknown, this peer is not being managed by CM” is shown for the name and “Unknown” is displayed for the IP address.

Note The WAAS Central Manager device does not have any peers because it does not participate with any WAEs to optimize traffic. For this reason, the topology feature is not available on the WAAS Central Manager device.

Connection Trend Report

The Connection Trend Report displays the connection trends of applications on a device. The following charts are included:

- Optimized Connections Over Time, page 17-26
- Optimized vs Pass-Through Connections, page 17-26

Connections Statistics Report

The Connections Statistics report displays a Connections Statistics table for the device. The table displays all the TCP connections handled by the device and corresponds to the **show statistics connection** EXEC mode command in WAE and the **show waas connection brief** command in WAAS Express.

You can choose to display a subset of connections identified by IP address and port by filling in values in the Source/Destination IP Address and Source/Destination Port fields above the table and clicking Submit. To see the Connection Start Time for the active connections in appropriate time zones, you can select the time zone from the available values of CM Local Time, Device Local Time and UTC in the Show Connection Start Time field.

Note In case of a clock /timezone change in the WAE, the exact time for device timezone is reflected after the configuration synchronization cycles.

The table displays the following information about each connection:

- Source IP address and port.
- Destination IP address and port.
- Peer ID—Hostname of the peer device.
- Applied Policy/Bypass Reason—Displays icons representing the applied optimization policies, including TFO, DRE, LZ, and an application accelerator, respectively (hover your mouse over the icon to see its meaning). If the connection was not optimized, the bypass reason is shown.
- Connection Start Time—Date and time when the connection was started.
- Open Duration—Number of hours, minutes, and seconds that the connection has been open.
- Total number of original bytes.
- Total number of optimized bytes.
- Percentage of compression.
- Class map name—If no class map exists for the connection, this column contains a dash. To create a class map for this connection, click the radio button at the left of the row and then click the **Create Class-Map** taskbar icon to display the Optimization Class-Map pane. For details on creating a class map and match conditions, see the chapter "Configuring Application Acceleration."

Note If the WAE is inheriting policies from a device group, the Create Class-Map button is not available, to prevent a user from unknowingly overriding device group policies. To create a class map, you must first override the device group policy page and then return to the Connection Statistics report.

The data in the Connections Statistics table is retrieved from the device one time when you view the window for the first time.

From the Connections Statistics table, you may perform the following tasks:

- Apply filter settings to display particular connections based on criteria that you choose, by choosing Quick Filter from the Show drop-list in the taskbar.
- Refresh the table by clicking the **Refresh** taskbar icon.
- Export the table to a spreadsheet by clicking the **Export** taskbar icon.
- View connection details by clicking the the **Details** icon next to the connection entry.

The Connection Details window contains connection addresses, port information, policy information, and traffic statistics. The Connection Details window also displays graphs that plot real-time traffic statistics and are refreshed every two seconds.

Note In the Connection Details window, if the value for Percentage Compression is negative, the Percentage Compression and Effective Capacity values do not appear.

In some cases, the Central Manager is not able to fetch the Connections Statistics page details at the WAE device level. This happens when the WAE uses internal ip for management purpose with the CM and external ip (NAT) for RPC or registration purpose with the WAAS Central Manager, and if that internal ip not reachable from the WAAS Central Manager.

CIFS Acceleration Report

The CIFS Acceleration report displays the CIFS acceleration statistics for a WAAS device. The following charts are included on two tabs:

- CIFS: Connection Statistics—Displays the number of CIFS accelerated sessions.
- CIFS: File Optimization—Displays the number of open CIFS files.
- CIFS: Request Optimization—Displays the percentage of requests that are served locally from the CIFS cache.
- CIFS: Cache Utilization—Displays the utilization percentage of the CIFS cache.
- CIFS: Cached Objects—Displays the number of objects in the CIFS cache.
- CIFS: Client Average Throughput—Displays the average throughput (in KB/second) between the WAAS device and its clients.

Note When you use the Print icon in the taskbar to print the CIFS Acceleration report to a file, all the CIFS charts will display the time in WAE local time (the CE Local Time setting), regardless of the chart time zone settings that you have configured.

Note The CIFS Acceleration report is not available for ISR-WAAS devices.

Note If there are issues in the Adobe® Flash® charts showing up in the GUI, clear the browser cache and restart the browser.

CIFS Acceleration Report for WAAS Express

The CIFS Acceleration report for WAAS Express displays the CIFS acceleration statistics for a WAAS Express device. The following charts and tables are included:

- CIFS: Client Average Throughput, page 17-25
- CIFS: Connection Details, page 17-25
- CIFS: Effective WAN Capacity, page 17-25
- CIFS: Request Optimization, page 17-25
- CIFS Acceleration Statistics Table for WAAS Express, page 17-34

Resource Utilization Report

The Resource Utilization report displays the following charts:

- CPU Utilization
- Disk Utilization

Disks Report

The Disks Report displays physical and logical disk information.

The report window displays the following information about each disk:

- Physical disk information, including the disk name, serial number, and disk size.
- Present status. The Present field will show either Yes if the disk is present or Not Applicable if the disk is administratively shut down.
- Operational status (NORMAL, REBUILD, BAD, UNKNOWN, or Online).
- Administrative status (ENABLED or DISABLED). When the Administrative Status field shows DISABLED, the Present field will show Not Applicable.
- Current and future disk encryption status.
- Current and future extended object cache status.
- RAID level. For RAID-5 devices, the Disk Information window includes the RAID device name, RAID status, and RAID device size.
- Error information, if any errors are detected.

From this window, you may save all disk information details to an Excel spreadsheet by clicking the **Export Table** icon in the taskbar.

AppNav Report

The AppNav report displays AppNav flow distribution information. This report is available at the AppNav Cluster level, where it shows statistics for the whole AppNav Cluster, and at the device level for AppNav Controllers (ANCs), where it shows statistics for a single ANC.

The following charts and tables are included:

- Total AppNav Traffic, page 17-27
- AppNav Policies, page 17-27
- Top 10 AppNav Policies, page 17-27
- Top 10 WAAS Node Group Distribution, page 17-27
- WAAS Node Group Distribution, page 17-27
- Pass-Through Reasons, page 17-27
- Top 10 Pass-Through Reasons, page 17-27

At the AppNav Cluster level, the following additional controls appear in the taskbar:

- The Scope pull-down list allows you to choose to display data for the whole cluster or for an individual ANC.
- The AppNav Policy Rule pull-down list allows you to choose the AppNav policy for which data is displayed. (Shown for WAAS appliance AppNav clusters only.)
- The Context pull-down list allows you to choose the AppNav context (or all contexts) for which data is displayed. (Shown for AppNav-XE clusters only.)

Note At the AppNav Cluster level, the charts may not show data if the configuration on all ANCs in the cluster does not match. To resolve this situation, choose **AppNav Clusters** > *cluster-name* from the Central Manager menu and click the taskbar icon named Force Settings on all Devices in a Group. After about 15 minutes, the AppNav charts should display data.

Managing Reports

The WAAS Central Manager allows you to edit any of the predefined reports and to create custom reports. Additionally, you can schedule reports to be generated periodically such as hourly, daily, weekly, or monthly. When a scheduled report is generated, a link to the report is e-mailed to notify the recipients.

This section contains the following topics:

Creating Custom Reports

A report consists of up to eight charts and tables. The system and device dashboard displays are examples of predefined reports, along with the other reports available in the Monitor menu.

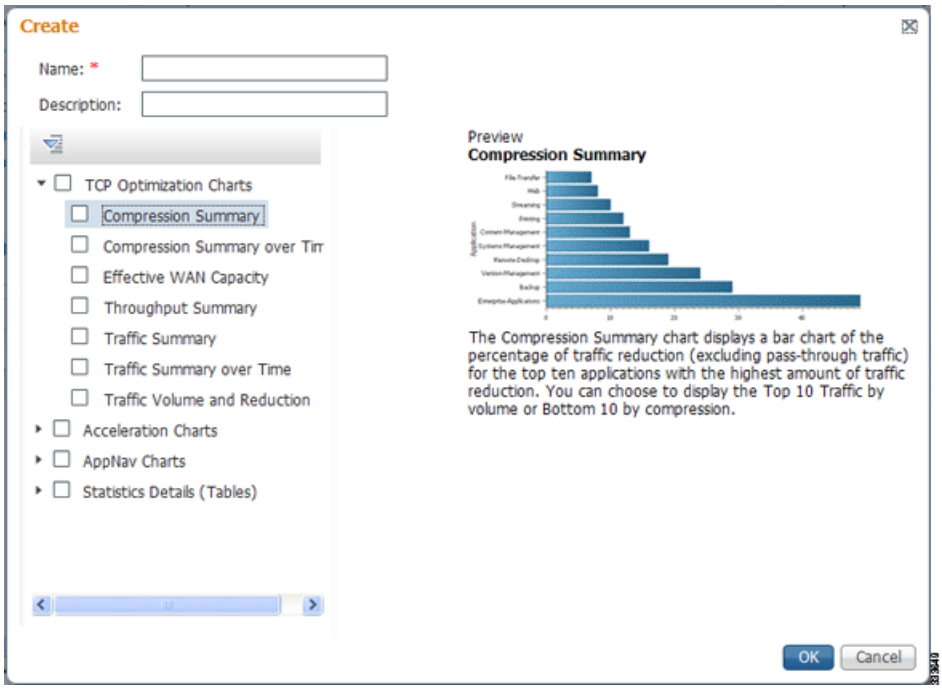
Reports can be created only at the system level, not at the device level.

To create a custom report, follow these steps:

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

Step 2 Click the **Create** taskbar icon. The Create Report pane appears, as shown in Figure 17-8.

Figure 17-8 Create Report Pane



Step 3 In the Name field, enter a name for the report using up to 64 characters. Only the following characters are allowed to be entered: numbers, letters, spaces, periods, hyphens, and underscores.

Step 4 (Optional) In the Description field, enter a description of the report.

Step 5 In the list at the left side of the pane, check the box next to each chart and table that you want to display in the report. See the "Chart and Table Descriptions" section on page 17-14 for a description of the charts.

Expand any of the categories by clicking on the small triangle next to the category name. See a preview and description of any chart by clicking on the chart name. Tables are listed in the last category, Statistics Details.

Step 6 Click **OK**.

Step 7 (Optional) Customize any of the chart settings as follows:

a. Display the report by clicking the report name in the Report Templates table. You may have to scroll the table.

b. You can customize report settings such as the time frame and the time zone as described in the "Customizing a Dashboard or Report" section on page 17-10.

c. Click the **Edit** icon in the upper left of a chart to customize the chart settings. For more information, see the "Configuring Chart Settings" section on page 17-14.

d. Click **OK**.

Repeat the steps for each chart you want to customize.

Another way you can create a report is to copy a similar existing report and modify it into a new report. To copy a report, follow these steps:

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

Step 2 Check the box next to the report that you want to copy.

Step 3 Click the **Copy** taskbar icon. The copy report window appears.

Step 4 In the Name field, enter a name for the report.

Step 5 (Optional) In the Description field, enter a description of the report.

Step 6 Click **OK**.

The report is added to the Reports table.

Viewing and Editing Reports

To view or edit a report, follow these steps:

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

Step 2 Click the name of the report that you want to view or edit.

If you do not see the report that you are looking for, you may need to scroll the Reports table. You can filter the list by choosing **Quick Filter** from the Show drop-down list and entering filter criteria.

Step 3 If you want to change any of the charts or tables in the report, use the standard chart editing methods as described in the "Customizing a Dashboard or Report" section on page 17-10.

Step 4 Click **Save** or **Save As** to save the report.

To delete a report from the Reports table, check the check box next to the report and click the **Delete** taskbar icon.

Admin users can view, edit, and delete reports created by all users and can view and edit predefined reports. Non-admin users can view, edit, and delete only reports created by themselves and can view and edit predefined reports.

Scheduling Reports

You can schedule reports to be generated once or periodically such as daily, weekly, or monthly. When a scheduled report is generated, a copy of the report can be e-mailed.

To schedule a report, follow these steps:

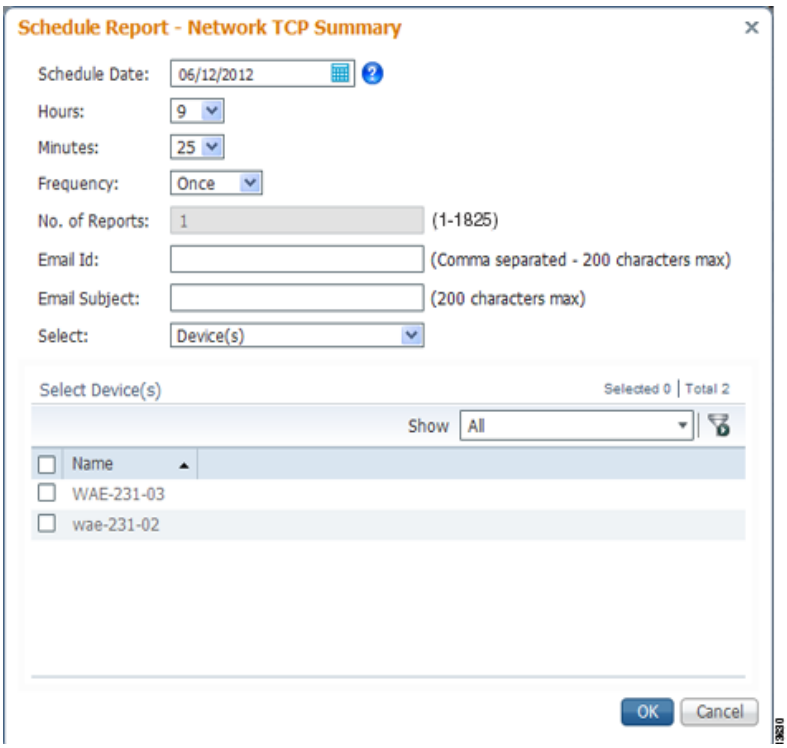
Step 1 From the WAAS Central Manager menu, choose **Monitor** > **Reports** > **Reports Central**.

Step 2 Check the box next to the report that you want to schedule.

If you do not see the report that you are looking for, you may need to scroll the Reports table.

Step 3 Click the **Schedule** icon in the taskbar. The scheduling window appears, as shown in Figure 17-9.

Figure 17-9 Scheduling a Report



Step 4 In the Date field, enter the schedule date in the format DD/MM/YYYY or click the calendar icon to display a calendar popup window from which to choose the date.

Step 5 In the Hours drop-down list, choose the hours. The time represents the local time at the WAAS Central Manager.

Step 6 In the Minutes drop-down list, choose the minutes. The time represents the local time at the WAAS Central Manager.

Step 7 In the Frequency drop-down list, choose Once, Hourly, Daily, Weekly, or Monthly for the report frequency.

Step 8 In the No. of Reports field, enter the number of times that a reoccurring report is to be generated. After being generated the specified number of times, the report is no longer generated.

Step 9 Select the Email PDF or Email CSV check box to receive the report format of your choice.

Step 10 In the Email Id field (enabled only when the above check boxes are selected), enter the e-mail addresses of the report recipients, separated by commas.

Step 11 In the Email Subject field, enter the subject of the e-mail message.

Step 12 In the Select drop-down list, choose **Device(s)**, **DeviceGroup**, **Cluster**, or **Location** to display a list of the chosen entities.

Step 13 In the Select entity area, choose the devices that are to be included in the statistics for the report. Place a check in the box next to each device, device group, cluster, or location that you want to include.

To find (highlight) an entity in a long list, choose **Quick Filter** from the Show drop-down list and enter the entity name (or partial name) in the field above the list. The search is case sensitive.

Step 14 Click **OK**.

Step 15 Configure the e-mail server settings for e-mail notification when reports are generated. For more information, see the "Configuring the E-mail Notification Server" section on page 10-24.

Note In a WAAS network where there are 1000 or more WAEs, a scheduled report might take up to 4 minutes to generate. And if you schedule more than one report at the same time, the reports will be generated with a delay of up to 20 minutes, depending on the number of reports and devices.

Managing Scheduled Reports

To view or delete a scheduled report, follow these steps:

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

The lower part of the Reports window lists the completed and pending scheduled reports, depending on which tab you choose. You can use the Show filter above the table to filter the reports that are displayed.

Step 2 (Optional) If you want to view a completed report instance in the Completed Reports tab, click the **Completed** link in the Status column.

Note For each completed instance of a scheduled report, the Frequency column shows Once and the Completed Time shows the date and time that the report was generated.

Step 3 (Optional) If you want to view a list of pending reports, click the **Pending Reports** tab.

Step 4 (Optional) If you want to delete a report in either the Completed Reports or Pending Reports tabs, check the box next to one or more report instances that you want to delete and click the **Delete** taskbar icon.

WAAS stores the 10 most recently completed or failed report instances for each custom report. This number is configurable by the System.monitoring.maxReports system property. For details on changing this property, see the "Modifying the Default System Configuration Properties" section on page 10-17.

Admin users can view reports scheduled by all users and the name of the report creator. Non-admin users can view only reports scheduled by themselves.

Any changes to predefined report settings are stored separately for individual users. That is, if one user changes a predefined scheduled report, only that user sees the changes, and other users (including admin users) continue to see the report with default settings.

Any reports scheduled by an external user are deleted if the maximum limit of days without a login passes and the user is deleted. For more information, see the cdm.remoteuser.deletionDaysLimit system configuration property in Table 10-4 on page 10-18.

Configuring Flow Monitoring

Flow monitoring applications collect traffic data that is used for application trend studies, network planning, and vendor-deployment impact studies. This section describes how to configure the flow monitoring feature on the WAE and includes the following topics:

- Configuring Flow Monitoring with NetFlow
- Configuring Flow Monitoring with NetQoS
- Alarms for Flow Monitoring, page 17-55
- Example Using NetQoS for Flow Monitoring, page 17-55

NetQoS

The NetQoS monitoring application can interoperate with the WAAS software to provide flow monitoring. To integrate this application with the WAAS software, you configure the NetQoS FlowAgent module on the WAE devices. The NetQoS FlowAgent module on the WAE collects important metrics of packet flows, which are then sent across the network to the NetQoS SuperAgent. This monitoring agent analyzes the data and generates reports. For this feature to work, additional configuration is required on the NetQoS FlowAgent. (See the "Example Using NetQoS for Flow Monitoring" section on page 17-55.)

The monitoring agent is composed of two modules: the console (or host) and the collector. The WAE initiates two types of connections to these two monitoring agent modules: a temporary connection to the console and a persistent connection to the collector. You configure the console IP address on the WAE by entering the **flow monitor tcpstat-v1 host** configuration mode command in either the WAE CLI or through the Central Manager GUI. This temporary connection is referred to as the control connection. The control connection uses TCP port 7878. Its purpose is to obtain the IP address and port number of the collector to which the WAE is assigned. The WAE also pulls the configuration information regarding which servers are to be monitored over the control connection. Once the WAE obtains the IP address and port number of the collector, the WAE opens a persistent connection to the collector. Collected summary data for the servers that are being monitored is sent over this persistent connection.

You may place the console (or host) module and the collector module on a single device or on separate devices. These connections are independent of one another. A failure of one connection does not cause the failure of the other connection and vice versa.

The state of these connections and various operation statistics display when you use the **show statistics flow monitor tcpstat-v1** EXEC mode command. Connection errors and data transfer errors trigger alarms on the WAE and in the Central Manager GUI. (See the "Alarms for Flow Monitoring" section on page 17-55.) To display debug information, use the **debug flow monitor tcpstat-v1** EXEC mode command.

To configure NetQoS flow monitoring on your WAEs using the Central Manager GUI, follow these steps:

Step 1 Create a new device group for configuring flow monitoring on multiple devices. Choose **Device Groups** > *device-group-name* > **Create New Device Group** to create a device group.

a. When you create the device group, check the **Automatically assign all newly activated devices to this group** check box to enable this option.

b. Add your existing WAE devices to this new device group.

Step 2 From the Device Group listing window, click the **Edit** icon next to the name of the flow monitoring configuration device group that you want to configure.

Step 3 Choose **Configure** > **Monitoring** > **Flow Monitor**. The Flow Monitor Settings for Device Group window appears.

Step 4 In the Destination IP Address field, enter the IP address of the monitoring agent console.

This configuration allows the WAE to establish a temporary connection (a control connection) to the console for the purpose of obtaining the IP address of the collector device. You must configure the collector IP address information from the console device. (See the configuration documentation for the NetQoS flow monitoring application software.)

Step 5 Check the **Enable Flow Monitor** check box.

Step 6 Click **Submit** to apply the settings to the devices in this device group.

To configure NetQoS flow monitoring on the WAE using the CLI, follow these steps:

Step 1 Register the WAE with the IP address of the monitoring agent console.

```
WAE(config)# flow monitor tcpstat-v1 host 10.1.2.3
```

This configuration allows the WAE to establish a temporary connection (a control connection) to the console (or host) for the purpose of obtaining the IP address of the collector device. You must configure the collector IP address information from the console device. (See the configuration documentation for the NetQoS flow monitoring application software.)

Step 2 Enable flow monitoring on the WAE appliance.

```
WAE(config)# flow monitor tcpstat-v1 enable
```

Step 3 Check the configuration by using the **show running-config** EXEC command.

NetFlow v9

NetFlow v9 is a template-based protocol developed by Cisco Systems to collect IP traffic information. The NetFlow v9 record format consists of a packet header followed by a template flowset of data flowset. A template flowset contains a description of the fields to be sent through in the data flowset. A data flowset is a collection of the data records containing flow information that is put into an export packet.

WAAS v5.3.1, NetFlow v9 provides the following features:

- Unlike NetFlow v5, which used a fixed format, NetFlow v9 utilizes a template format. All WAAS optimization engines can use this template format to export data to such collectors as Cisco NAM, Cisco Prime, and Solarwinds.
- The template format allows new features to be quickly added to NetFlow v9.
- Templates are checked every few minutes for changes, and sent out hourly to provide collectors with field information for data records.
- NetFlow v9 uses WAAS transaction log information and adds an exporter code to allow data to be sent to external devices.
- NetFlow v9 can be used on all WAAS optimization engines; it is not used with WAAS AppNav.
- By default, all WAAS class maps are monitored. If you would like to have specific class maps to not be monitored, see the Disabling NetFlow v9 section.

To configure NetFlow v9 on your WAEs with either the Central Manager GUI or the CLI, you configure four monitoring areas:

- Flow Record - Contains the WAAS-specific flow information you want to send to the collector.

- Flow Exporter - Contains the destination for the exported information, and the format for this information.
- Flow Monitor - Specifies which flow records are going to which flow exporter.
- Class Map - For WAAS 5.3.1, monitors are enabled globally on all class map policies by default. If you do not want a particular device monitored, manually disable monitoring for that device.

To configure NetFlow v9 flow monitoring on the WAE using the CLI, follow these steps:

Step 1 To create a flow record to configure the fields to collect as part of Netflow export:

```
WAE(config)# flow record RecordName
WAE(config)# collect waas ?
```

Collection Parameter	Description
application-name	Collect application name for the flow.
bytes	Collect byte counts for the flow.
class-name	Collect class name for the flow.
connection-mode	Collect connection mode for the flow.
dre	Collect DRE details for the flow.
lz	Collect LZ details for the flow.
packets	Collect packet counts for the flow.
passthrough-reason	Collect pass-through reason for the flow.

Step 2 To create the flow exporter, which includes the destination IP address and port for the Netflow:

```
WAE(config)# flow exporter ExporterName
WAE(config)# destination
WAE(config)# transport
WAE(config)# export-protocol NETFLOW-V9
WAE(config)# description
```

Step 3 To create the flow monitor, which enables flow monitoring on all classes:

```
WAE(config)# flow monitor type performance-monitor MonitorName
WAE(config)# exporter ExporterName
WAE(config)# record RecordName
WAE(config)# enable
```

Disabling NetFlow v9

By default, flow monitoring is enabled on all devices. To disable monitoring for a particular class:

```
WAE(config)# policy-map type waas PmapName
WAE(config)# class ClassName
WAE(config)# {no} flow-monitor enable
```

NetFlow v9 Exported Fields

In Netflow v9 there are several fields that can be provided to the Netflow collector. The following table provides some examples of these fields:

Exported Field	Description and Corresponding Number Value
Segment ID	The segment of the optimized flow that the values are from: 1, 2, 4, 8, or 16. A value of 1 is un-optimized side on the Edge WAE, and a value of 16 is a pass-through flow.
Source IP	Source IP address.
Destination IP	Destination IP address.
NextHop	IP address of next hop router.
Input Interface	SNMP index of input interface.
Output Interface	SNMP index of output interface.
Source Port	TCP/UDP source port number or equivalent.
Destination Port	TCP/UDP destination port number of equivalent.
TCP Flags	Cumulative OR of TCP flags.
Packets	Packets in the flow.
Bytes	Unused bytes.
Start Time	System uptime at start of flow.
End Time	System uptime when the last packet of the flow is received.
Protocol	IP protocol type (for example, TCP=6, UDP=17)
Type of Service	The type of service.
Source ASN	Autonomous System Number of the source, either origin or peer.
Destination ASN	Autonomous System Number of the destination, either origin or peer.
Source Mask	Source address of the prefix mask, in bits.
Destination Mask	Destination address of the prefix mask, in bits.
Application Name	Name of the application traffic on the connection.
Class Name	The class name.
Connection Mode	The current connection mode: A value of 1 (TFO), 3 (TFO + DRE), 5 (TFO + LZ) or 7 (TFO + DRE + LZ).
Pass-Through Reason	Reason traffic was not optimized.
Bytes Received	Number of bytes received.
Bytes Sent	Number of bytes sent.
Packets Received	Number of packets received.
Packets Sent	Number of packets sent.
DRE In Bytes	Number of DRE bytes before compression.
DRE Out Bytes	Number of DRE bytes after compression.
DRE Encode Latency	Amount of latency incurred during DRE encode operation against an optimized connection.

DRE Decode Latency	Amount of latency incurred during DRE decode operation against an optimized connection.
LZ In Bytes	Number of LZ bytes before compression.
LZ Out Bytes	Number of LZ bytes after decompression.
LZ Encode Latency	The amount of latency (transmission delay) associated with the LZ compressed message operation.
LZ Decode Latency	The amount of latency (transmission delay) associated with the LZ decompressed message operation.
Original Bytes	Number of unoptimized bytes.
Optimized Bytes	Number of optimized bytes.

NetFlow v9 Pass-Through Reasons

Pass-Through reasons are sent to the collector; this table provides pass-through numbers and associated reasons.

Pass-Through Number	Pass-Through Reason
0	PE_CONN_UNKNOWN
1	PE_CONN_PT_APP_CONFIG
2	PE_CONN_PT_GLB_CONFIG
3	PE_CONN_PT_OVERLOAD
4	PE_CONN_PT_CPU_OVERLOAD
5	PE_CONN_PT_IN_PROGRESS
6	PE_CONN_PT_PE_INT_ERROR
7	PE_CONN_PT_DYN_BYPASS
8	PE_CONN_INT_CLIENT
9	PE_CONN_INT_SERVER
10	PE_CONN_ACCEL_OPTIMIZED
11	PE_CONN_ACCEL_NON_OPTIMIZED
12	PE_CONN_APP_DYN_MITCH_OPTIMIZED
13	PE_CONN_APP_DYN_MITCH_NON_OPTIMIZED
14	PE_CONN_OPT_TCP_PLUS
15	PE_CONN_ORIG_TCP_PLUS
16	PE_CONN_OPT_PREPOSITION
17	PE_CONN_ORIG_PREPOSITION
18	PE_CONN_OPT_TCP_ONLY
19	PE_CONN_ORIGIN_TCP_ONLY
20	PE_CONN_PT_NO_PEER
21	PE_CONN_PT_RJCT_CAPABILITIES
22	PE_CONN_PT_RJCT_RESOURCES

23	PE_CONN_PT_NO_LICENSE
24	PE_CONN_PT_ASYMMETRIC
25	PE_CONN_PT_INTERMEDIATE
26	PE_CONN_PT_FB_INT_ERROR
27	PE_CONN_PT_AD_INT_ERROR
28	PE_CONN_PT_SQ_INT_ERROR
29	PE_CONN_PT_APP_OVERRIDE
30	PE_CONN_PT_SVR_BLACKLIST
31	PE_CONN_PT_AD_VER_MISMATCH
32	PE_CONN_PT_AD_AO_INCOMPAT
33	PE_CONN_PT_AD_AOIM_PROGRESS
34	PE_CONN_PT_DIRM_VER_MISMATCH
35	PE_CONN_PT_DIRM_INT_ERROR
36	PE_CONN_PT_PEER_OVERRIDE
37	PE_CONN_PT_AD_OPT_PARSE_FAIL
38	PE_CONN_PT_AD_SERIAL_MODE_PEER
39	PE_CONN_PT_INTERCEPTION_ACL
40	PE_CONN_PT_WCCP_SHUTDOWN_ACTIVE
41	PE_CONN_PT_AD_IP_FRAG

Troubleshooting Flow Monitoring

To troubleshoot flow monitor information, use the following commands:

Command Type	Command
show commands	# **show flow record RecordName** # **show flow record RecordName template** # **show flow ExporterName exporter** # **show flow monitor**
show statistics commands	# **show statistics flow monitor MonitorName** # **show statistics flow exporter ExporterName**
clear statistics commands	# **clear statistics flow monitor MonitorName** # **clear statistics flow exporter ExporterName**
tcpdump command	# **tcpdump**

Alarms for Flow Monitoring

Table 17-15 describes the four different alarms that may be raised when errors occur with flow monitoring.

Table 17-15 Alarms for Flow Monitoring

Name	Severity	Description
CONTROL_CONN	Major	Indicates a problem with the control connection.
COLLECTOR_CONN	Major	Indicates a problem with the collector connection.
SUMMARY_COLLECTION	Minor	Indicates a problem with the collection of packet summary information. Summary packets may be dropped because the buffer queue limit has been reached or because of a TFO error, such as not being able to allocate memory. Summary packet collection may also be dependent on available WAN bandwidth.
DATA_UPDATE	Minor	Indicates a problem with the ability of the WAE to send updates the collector agent.

Example Using NetQoS for Flow Monitoring

NetQoS integrates with the WAAS software by running the NetQoS FlowAgent on WAE devices. FlowAgent is a software module developed by NetQoS that resides on the WAE appliance. The FlowAgent collects metrics about the packet flows, which are then sent across the network to a NetQoS SuperAgent. The SuperAgent measures the round-trip times, server response times, and data transfer times, and then analyzes the data and generates reports.

Note When you use flow monitoring with the NetQoS SuperAgent, the flow monitor on the WAE captures optimized traffic only.

To configure flow monitoring with NetQoS, follow these steps:

Step 1 From the WAE CLI or Central Manager GUI, enter the SuperAgent Master Console IP address in the Destination IP Address field on your WAE appliances.

If you are configuring multiple WAAS devices through a device group, wait for the configuration to propagate to all the devices in the device list.

Step 2 From the NetQoS SuperAgent console, assign a WAE to a SuperAgent Aggregator (known as the collector in WAAS terminology) and configure the NetQoS Networks, Servers, and Applications entities.

Note For information about using the NetQoS SuperAgent Master Console and configuring NetQoS SuperAgent entities, go to the following website: http://support.ca.com

Configuring and Viewing Logs

This section contains the following topics:

Configuring System Logging

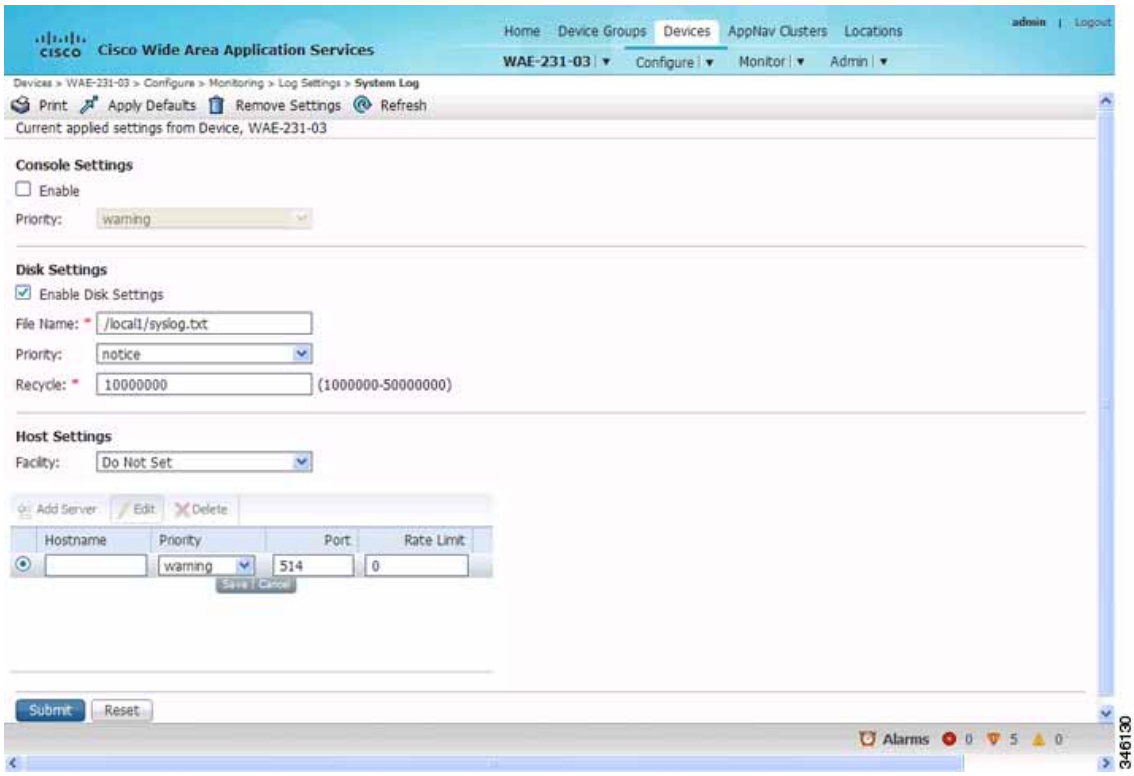
Use the WAAS system logging feature to set specific parameters for the system log file (syslog). This file contains authentication entries, privilege level settings, and administrative details. The system log file is located on the system file system (sysfs) partition as /local1/syslog.txt.

To enable system logging, follow these steps:

Step 1 From the WAAS Central Manager 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 17-10.)

Figure 17-10 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 17-16 on page 17-58 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 17-16 on page 17-58 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 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 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, see the "Multiple Hosts for System Logging" section on page 17-59.

c. In the Hostname field, enter a hostname or IP address 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 17-16 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

Table 17-16 lists the different priority levels of detail to send to the recipient of the syslog messages for a corresponding event.

Table 17-16 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:

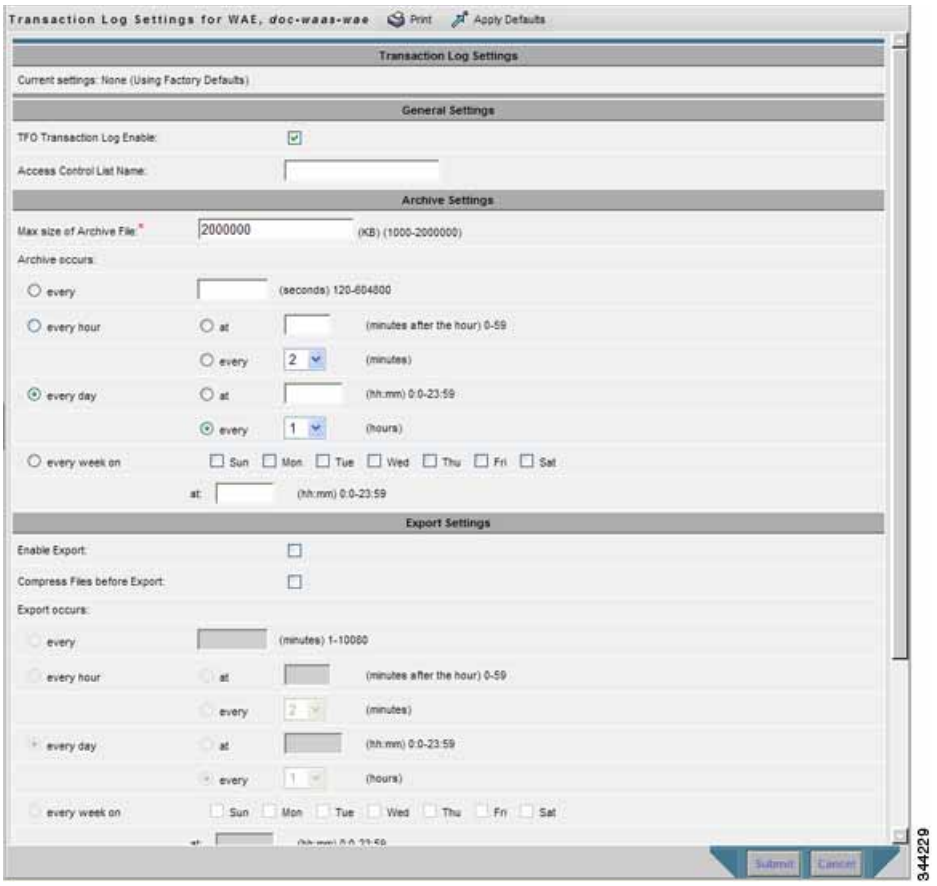
Enabling Transaction Logging

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 17-11.) The Video Transaction Log Settings window looks the same, but does not include the General Settings area at the top.

Figure 17-11 Transaction Log Settings Window



Step 3 Under the General Settings heading, 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 In the Access Control List Name field, optionally 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 the 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 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 6 Configure the fields in the Export Settings section to export the transaction log file to an FTP server.

Table 17-17 describes the fields in the Export Settings section.

Table 17-17 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 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** global configuration command.

Transaction Logs

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

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 directory /local1/logs/.

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 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 messages from registered devices with a severity level of "warning" or higher.

To view logged information for 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, the name displayed is "Unavailable." This situation might occur if the node has been deleted or has been reregistered with the WAAS software.

Step 2 (Optional) Choose **Quick Filter** in 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 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 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 from the log that match the specified pattern.

c. Click **OK** when 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 logged activites 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** in 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 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 17-62.

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** in 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.

Troubleshooting Tools

This section contains the following topics:

For additional advanced WAAS troubleshooting information, see the *Cisco WAAS Troubleshooting Guide for Release 4.1.3 and Later* on Cisco DocWiki.

Enabling the Kernel Debugger

The WAAS Central Manager GUI allows you to enable or disable access to the kernel debugger (kdb). Once 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 Diagnostic Tests

WAAS includes diagnostic testing tools as described in the following sections:

- Diagnostic Testing Using the GUI, page 17-64
- Diagnostic Testing Using the CLI, page 17-65

Diagnostic Testing Using the GUI

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 that you want to run, or check the top check box to run all tests. The following tests are available:

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

Note A Virtual Interface test is available for vWAAS devices.

- Configuration Security—Check the running configuration for potentially malicious (XSS) entries.
- Traffic Optimization—Check the TFO configuration and operation.
- WCCP configuration and operation—Check the configuration and operation of WCCP traffic interception.
- Inline configuration and operation—Check 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. You may have to scroll the window to see all results.

For tests that 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.

Diagnostic Testing Using the CLI

You can use the **test** EXEC command to perform diagnostic and connectivity tests.

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.

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.

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

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 any **debug** command, system logging must be enabled. The command to enable logging is the **logging disk enable** global configuration command, which 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, as follows:

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

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

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

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 menu, choose **Devices** > *device-name*.

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

Step 3 From the drop-down list, choose 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 appears, displaying the command output for that device.

The **show** and **clear** CLI commands that are available differ depending on the type of device that is selected.

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

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 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 context.)

Step 3 In the Destination IP and Destination Port fields, enter the IP address and port of the destination to 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. Use the filter settings in the Show drop-down list to filter the devices as needed. You can use a quick filter to filter on any value or show all devices.

You can display 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 the "AppNav Connection Tracing" section on page 4-51.