Cisco Wide Area Application Services Monitoring Guide

Software Version 5.0.1
November 14, 2012

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

Text Part Number: OL-26583-01

Cisco Wide Area Application Services Monitoring Guide

CONTENTS

Preface

This preface describes the audience, organization, and conventions of the *Cisco Wide Area Application Services Monitoring Guide*. It also provides information about how to obtain related information.

Audience

This publication is for experienced system and network administrators who have specific knowledge in the following areas:

- Networking and data communications
- Network security
- Router and switch configuration

Organization

This publication is organized as follows:

Chapter	Description
Chapter 1, "Monitoring WAAS Using WAAS Central Manager"	Describes how to use WAAS Central Manager to monitor your WAAS devices.
Chapter 2, "Monitoring Traffic Interception"	Describes different methods to monitor traffic interception.
Chapter 3, "Monitoring WAAS Using SNMP"	Describes how to use SNMP to monitor your WAAS devices.
Chapter 4, "Monitoring WAAS Using XML API"	Describes how to use WAAS XML API to monitor your WAAS devices.
Chapter 5, "Monitoring WAAS Using Cisco Network Analysis Module"	Describes how to use Cisco Network Analysis to monitor your WAAS devices.

Conventions

This document uses the following conventions:

Item	Convention
Commands and keywords	**boldface** font
Variables for which you supply values	*italic* font
Displayed session and system information	`screen` font
Information you enter	**`boldface screen`** `font`
Variables you enter	*`italic screen`* font
Menu items and button names	**boldface** font
Selecting a menu item in paragraphs	**Option > Network Preferences**
Selecting a menu item in tables	Option > Network Preferences

Note Means *reader take note*. Notes contain helpful suggestions or references to material not covered in the publication.

Caution Means *reader be careful*. In this situation, you might do something that could result in equipment damage or loss of data.

Related Documentation

For additional information on the Cisco WAAS software and hardware, see the following documentation:

- *Release Note for Cisco Wide Area Application Services*
- *Cisco Wide Area Application Services Upgrade Guide*
- *Cisco Wide Area Application Services Command Reference*
- *Cisco Wide Area Application Services Quick Configuration Guide*
- *Cisco Wide Area Application Services Configuration Guide*
- *Cisco Wide Area Application Services API Reference*
- *Cisco WAAS Troubleshooting Guide for Release 4.1.3 and Later*
- *Cisco Wide Area Application Services Monitoring Guide* (this manual)
- *Cisco Wide Area Application Services vWAAS Installation and Configuration Guide*
- *Cisco WAAS Installation and Configuration Guide for Windows on a Virtual Blade*
- *Configuring WAAS Express*
- *Cisco WAAS on Service Modules for Cisco Access Routers*
- *Cisco SRE Service Module Configuration and Installation Guide*
- *Configuring Cisco WAAS Network Modules for Cisco Access Routers*
- *WAAS Enhanced Network Modules*
- *Regulatory Compliance and Safety Information for the Cisco Wide Area Virtualization Engines*
- *Cisco Wide Area Virtualization Engine 294 Hardware Installation Guide*
- *Cisco Wide Area Virtualization Engine 594 and 694 Hardware Installation Guide*
- *Cisco Wide Area Virtualization Engine 7541, 7571, and 8541 Hardware Installation Guide*
- *Cisco Wide Area Virtualization Engine 274 and 474 Hardware Installation Guide*
- *Cisco Wide Area Virtualization Engine 574 Hardware Installation Guide*
- *Regulatory Compliance and Safety Information for the Cisco Content Networking Product Series*
- *Cisco Wide Area Application Engine 7341, 7371, and 674 Hardware Installation Guide*
- *Installing the Cisco WAE Inline Network Adapter*

Obtaining Documentation and Submitting a Service Request

For information about obtaining documentation, submitting a service request, and gathering additional information, see the monthly *What's New in Cisco Product Documentation*, which also lists all new and revised Cisco technical documentation, at:

http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html

Subscribe to the *What's New in Cisco Product Documentation* as a Really Simple Syndication (RSS) feed and set content to be delivered directly to your desktop using a reader application. The RSS feeds are a free service and Cisco currently supports RSS version 2.0.

CHAPTER 1

Monitoring WAAS Using WAAS Central Manager

This chapter describes how to use WAAS Central Manager to monitor network health, device health, and traffic interception of your WAAS system.

This chapter contains the following sections:

For more information about using WAAS Central Manager, see the “Monitoring and Troubleshooting Your WAAS Network” chapter in the *Cisco Wide Area Application Services Configuration Guide*.

Accessing the Central Manager

From a secure web browser, log in to WAAS Central Manager using either its hostname or IP address on port 8443 as follows:

https://*CM-Host-Name_or_IP Address*:8443

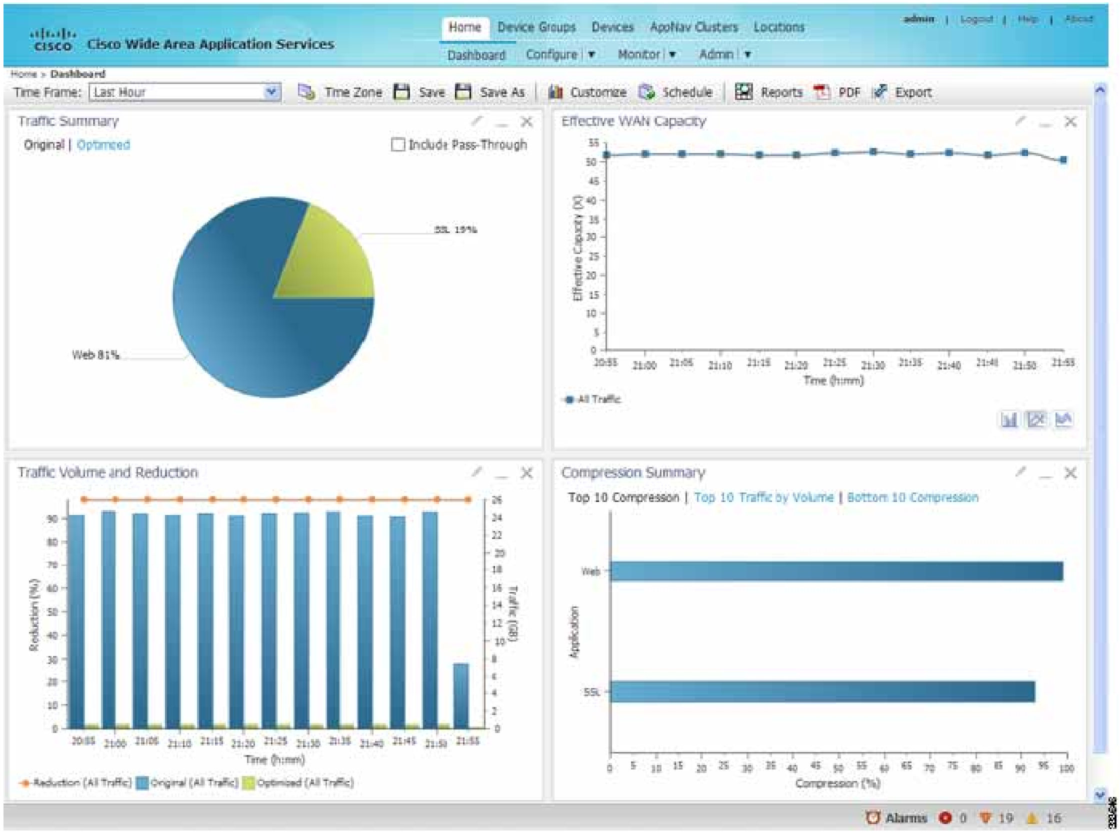
You must have proper username and password credentials to log in to WAAS Central Manager.

You initially open to a view of the WAAS System Dashboard, from which you can monitor your WAAS system. When you choose a device from the Devices menu, you move to the a view of the Device Dashboard, from which you can monitor specific device activity and performance.

Using the WAAS System Dashboard

The WAAS Central Manager GUI allows you to view general and detailed information about your WAAS network from the System Dashboard window, which is shown in Figure 1-1.

Figure 1-1 System Dashboard Window



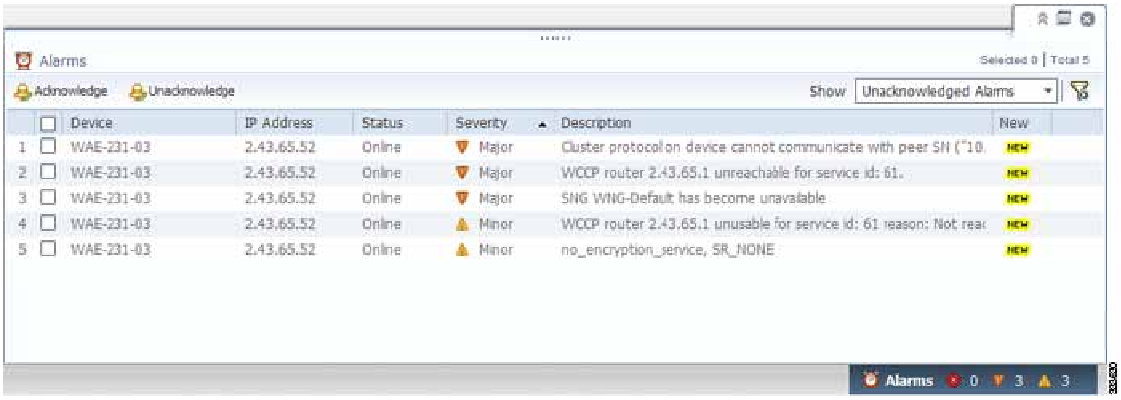
The dashboard provides a snapshot of your WAAS network. You can use the menu at the top of the dashboard window to view more detailed information about your devices, and to configure, monitor, and administer your network.

The Alarms section of the dashboard, in the gray status bar area at the bottom right of the window, provides instant access to any alarms, as described in the “Viewing Alarms” section on page 1-2.

Viewing Alarms

The Alarms panel at the bottom right side of the Central Manager window provides a near real-time view of incoming alarms and refreshes every two minutes to reflect updates to the system alarm database. The alarms are classified as Critical, Major, or Minor depending on the impact the issue might have upon the WAAS environment. You can click **Alarms** to display the panel, which is shown in Figure 1-2.

Figure 1-2 Alarms Panel



Selected 0 | Total 5

Show: Unacknowledged Alarms

	□	Device	IP Address	Status	Severity	Description	New
1	□	WAE-231-03	2.43.65.52	Online	Major	Cluster protocol on device cannot communicate with peer SN ("10	NEW
2	□	WAE-231-03	2.43.65.52	Online	Major	WCCP router 2.43.65.1 unreachable for service id: 61.	NEW
3	□	WAE-231-03	2.43.65.52	Online	Major	SNG WNG-Default has become unavailable	NEW
4	□	WAE-231-03	2.43.65.52	Online	Minor	WCCP router 2.43.65.1 unusable for service id: 61 reason: Not rea	NEW
5	□	WAE-231-03	2.43.65.52	Online	Minor	no_encryption_service, SR_NONE	NEW

The Alarms panel contains a filtering option that allows you to control which alarms are shown in the panel. You can check the check box next to an alarm name, and then click the **Acknowledge** taskbar icon to enter any comments you have about the alarm.

For a complete list of alarm conditions, see the *Alarm Book* located in the WAAS Software Download area on Cisco.com.

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 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, and provides menu access to reports and other information about the device.

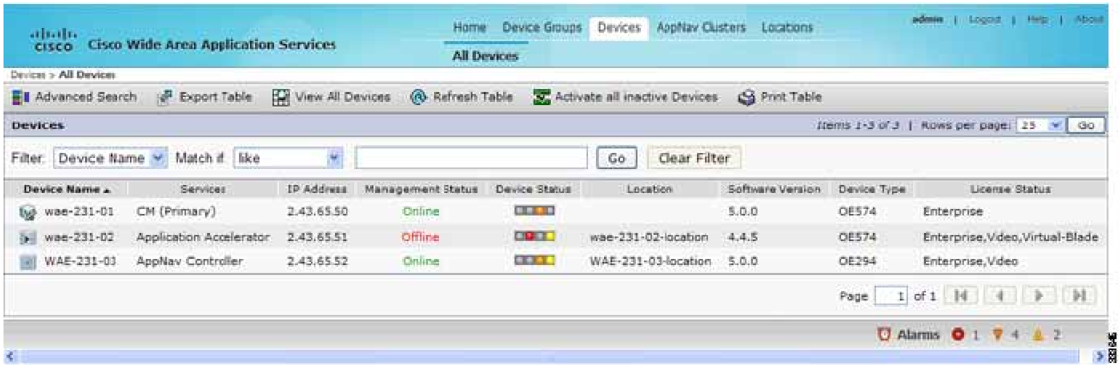
Devices Window

The Devices window displays a list of all the devices in your WAAS network with basic information about each device such as the device status and the current software version installed on the device. You can use either of these actions to display the Devices window:

- Click the **Devices** menu in the Central Manager window.
- Roll over the Devices menu in the Central Manager window and click **All Devices**.

An example of the Devices window is shown in Figure 1-3.

Figure 1-3 *Devices Window*



Devices — Items 1-3 of 3 | Rows per page: 25 Go

Filter: Device Name Match if like

Device Name ▲	Services	IP Address	Management Status	Device Status	Location	Software Version	Device Type	License Status
wae-231-01	CM (Primary)	2.43.65.50	Online			5.0.0	OE574	Enterprise
wae-231-02	Application Accelerator	2.43.65.51	Offline		wae-231-02-location	4.4.5	OE574	Enterprise,Video,Virtual-Blade
WAE-231-03	AppNav Controller	2.43.65.52	Online		WAE-231-03-location	5.0.0	OE294	Enterprise,Video

Page 1 of 1

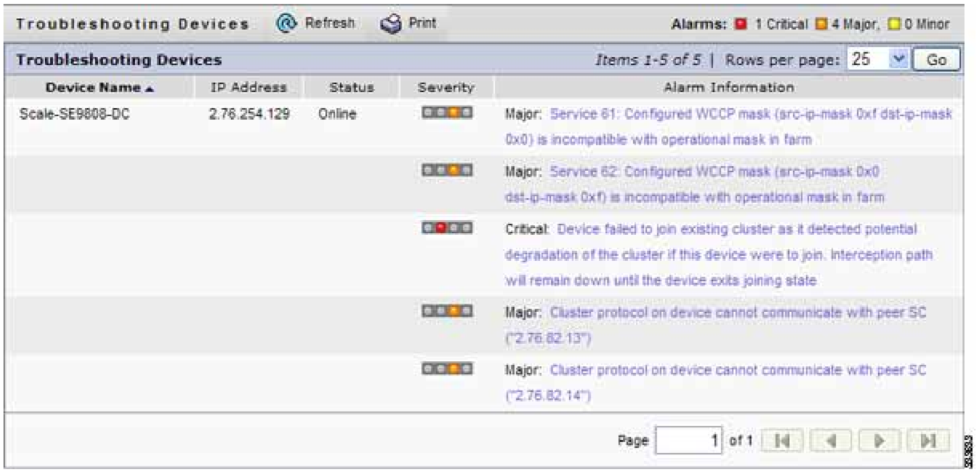
This window displays information about each device, including its management status, which is one of the following: Online, Offline, Pending, or Inactive. If a device's status is offline, you can use the command-line interface to verify its status and its participation in traffic optimization. For more information, see the "Running CLI Commands from the WAAS Central Manager GUI" section on page 1-16.

The Devices window also displays the device status for each device in your network in an alarm light bar, which has one of the following values:

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

If the device status is anything other than green, you can roll over the light bar to see a popup message with further details about the status. If you click the popup message, the Troubleshooting Devices window is displayed (see Figure 1-4).

Figure 1-4 *Troubleshooting Devices Window*



Troubleshooting Devices — Items 1-5 of 5 | Rows per page: 25 Go

Device Name ▲	IP Address	Status	Severity	Alarm Information
Scale-SE9808-DC	2.76.254.129	Online		Major: Service 61: Configured WCCP mask (src-ip-mask 0xf dst-ip-mask 0x0) is incompatible with operational mask in farm
				Major: Service 62: Configured WCCP mask (src-ip-mask 0x0 dst-ip-mask 0xf) is incompatible with operational mask in farm
				Critical: Device failed to join existing cluster as it detected potential degradation of the cluster if this device were to join. Interception path will remain down until the device exits joining state
				Major: Cluster protocol on device cannot communicate with peer SC ("2.76.82.13")
				Major: Cluster protocol on device cannot communicate with peer SC ("2.76.82.14")

Page 1 of 1

When you roll over an Alarm Information message, a set of troubleshooting links displays in the top part of the window to help you with tracking down the problem. Table 1-1 shows the links you may see.

Table 1-1 Troubleshooting Tools for Device Alarms

Item	Description
Update Software	Displays the Software Update window for this device. This link appears only if the device software version is lower than the Central Manager.
Edit/Monitor Device	Displays the Device Dashboard window for configuration.
Telnet to Device	Initiates a Telnet session using the device IP address.
View Device Log	Displays system message logs filtered for this device.
Run Show Commands	Displays the device **show** command tool. For more information, see the "Running CLI Commands from the WAAS Central Manager GUI" section on page 1-16.

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

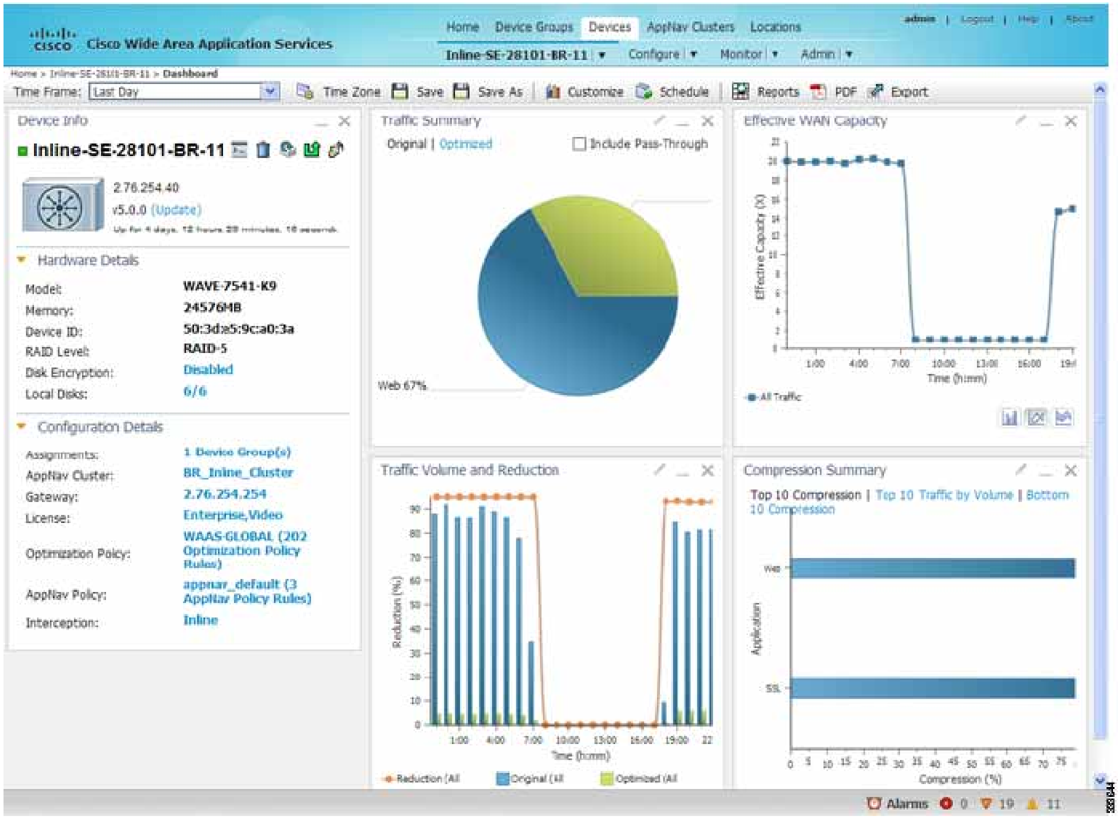
Device Dashboard Window

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 1-5.)

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

Note When you are using the Device Dashboard, the menu choices that are available are different than when you are using the System Dashboard.

Figure 1-5   Device Dashboard Window



Cisco Wide Area Application Services
Home | Device Groups | Devices | AppNav Clusters | Locations
admin | Logout | Help | About
Inline-SE-28101-BR-11 ▾ | Configure ▾ | Monitor ▾ | Admin ▾
Home > Inline-SE-28101-BR-11 > Dashboard
Time Zone | Save | Save As | Customize | Schedule | Reports | PDF | Export
Device Info
Hardware Details
Configuration Details
Traffic Summary
Original | Optimized
Include Pass-Through
Web 67%
Effective WAN Capacity
Effective Capacity (X)
Time (h:mm)
All Traffic
Traffic Volume and Reduction
Reduction (%)
Time (h:mm)
Reduction (All | Original (All | Optimized (All
Compression Summary
Top 10 Compression | Top 10 Traffic by Volume | Bottom 10 Compression
Application
Web
SSL
Compression (%)
Alarms 0 19 11

Time Frame: Last Day

Inline-SE-28101-BR-11

2.76.254.40
v5.0.0 (Update)

Model:	WAVE-7541-K9
Memory:	24576MB
Device ID:	50:3d:e5:9c:a0:3a
RAID Level:	RAID-5
Disk Encryption:	Disabled
Local Disks:	6/6
Assignments:	1 Device Group(s)
AppNav Cluster:	BR_Inline_Cluster
Gateway:	2.76.254.254
License:	Enterprise,Video
Optimization Policy:	WAAS-GLOBAL (202 Optimization Policy Rules)
AppNav Policy:	appnav_default (3 AppNav Policy Rules)
Interception:	Inline

The Device Dashboard window provides an overview of the device, including hardware and configuration details, and summaries of its traffic and compression statistics. You can initiate a number of device-specific actions from this window, including:

- Click the **Update** link (if shown) to update the software on the device.
- Click the **Telnet** icon to establish a Telnet session into the device and issue CLI commands.
- Click other icons to delete, reboot, or update the configuration of the device.
- Click the *Device-Name* menu and then select actions such as assigning the device to a device group or viewing and unlocking which users have access to the device.
- Click the **Edit** icon in a chart to modify which data is shown.
- Click the **Customize** icon in the task bar to customize charts and reports.

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

Viewing Monitoring Reports

The WAAS Central Manager GUI provides access to a number of reports you can use to monitor your network. Some reports display system-wide monitoring information, while others are only available from the Device Dashboard to display device-specific information.

This section contains the following topics:

- Viewing Network Reports, page 1-7
- Viewing Optimization Reports, page 1-9
- Viewing Acceleration Reports, page 1-11
- Viewing AppNav Reports, page 1-12
- Viewing Platform Reports, page 1-13

For more information about the available monitoring reports, see the "Monitoring and Troubleshooting Your WAAS Network" chapter in the *Cisco Wide Area Application Services Configuration Guide*.

Viewing Network Reports

You can monitor overall system information in the WAAS Central Manager GUI with several system-level reports. This section provides examples of these reports:

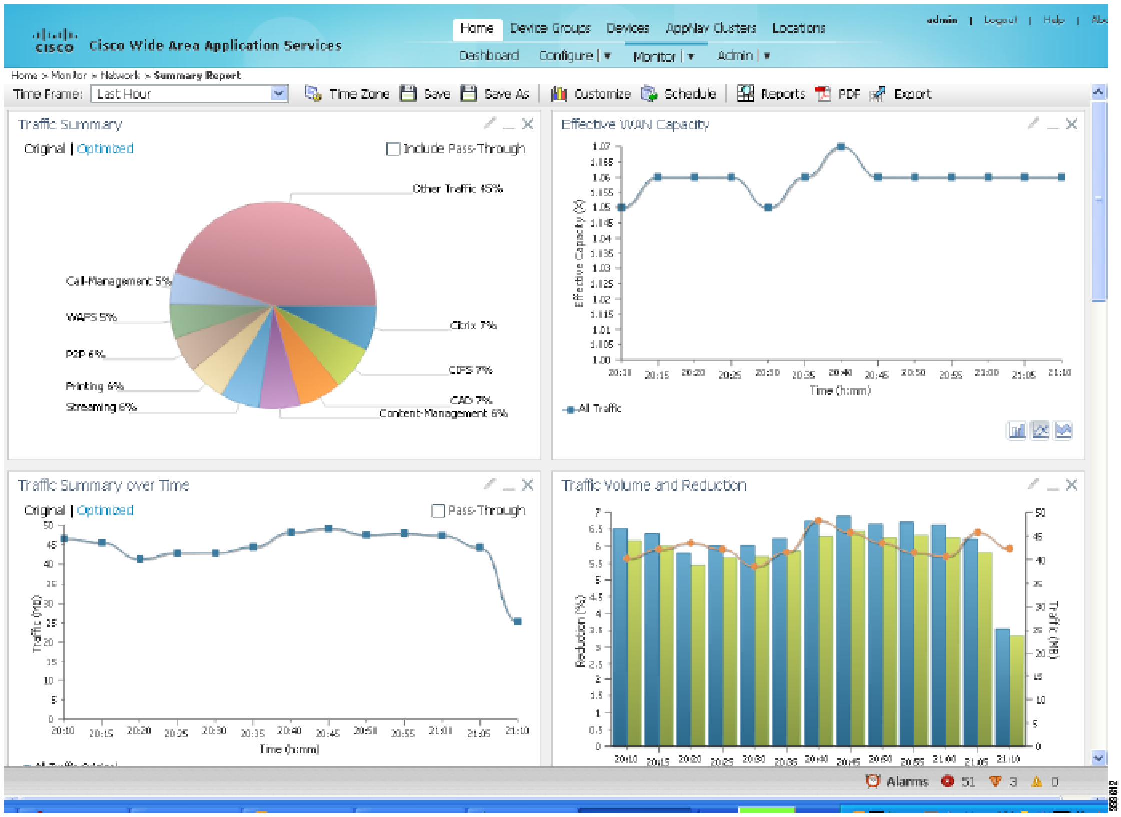
- Viewing Network Summary Information, page 1-7
- Viewing Network Topology, page 1-8

For more information, see the "Monitoring and Troubleshooting Your WAAS Network" chapter in the *Cisco Wide Area Application Services Configuration Guide*.

Viewing Network Summary Information

The Network Summary Report provides you with an overall view of network health and performance. To display this report, choose **Monitor** > **Network** > **Summary Report** in the System Dashboard. Figure 1-6 shows an example report.

Figure 1-6 Network Summary Report



Time Frame: Last Hour

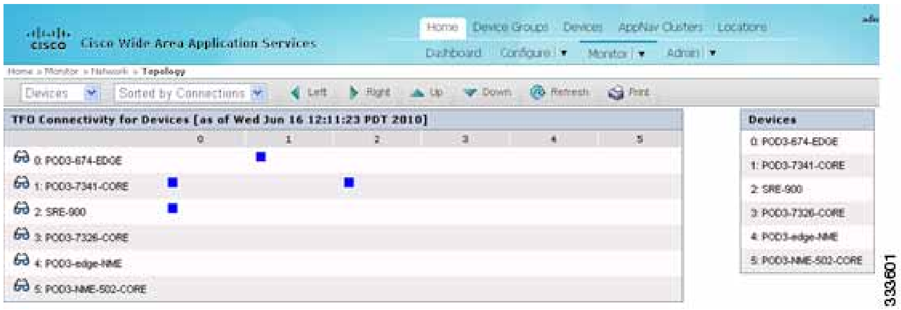
The Network Summary Report includes summary information about traffic, capacity, compression, and network applications.

Viewing Network Topology

You can use the Network Topology Report (see Figure 1-7) at the system level to display a graphical representation of all connections between WAAS devices. At the device level, the topology report lists all peer devices connected to a specific WAE, so you can see the relationship between devices in your WAAS network.

To view this report, choose **Monitor** > **Network** > **Topology** in either the System Dashboard or the Device Dashboard.

Figure 1-7 Topology Report



TFO Connectivity for Devices [as of Wed Jun 16 12:11:23 PDT 2010]

	0	1	2	3	4	5
0: POD3-674-EDGE		■				
1: POD3-7341-CORE	■		■			
2: SRE-900	■					
3: POD3-7326-CORE						
4: POD3-edge-NME						
5: POD3-NME-502-CORE						

Devices
0: POD3-674-EDGE
1: POD3-7341-CORE
2: SRE-900
3: POD3-7326-CORE
4: POD3-edge-NME
5: POD3-NME-502-CORE

The topology information is important for troubleshooting and for deployment-sizing exercises, especially for large deployments where any site-to-site communication is required.

Viewing Optimization Reports

You can view connection optimization statistics for your network connections in the Central Manager GUI. This section contains the following topics:

- Viewing TCP Statistics, page 1-9
- Viewing Connection Statistics, page 1-9
- Viewing Connection Trends, page 1-11

For more information about optimization statistics and reports, see the "Monitoring and Troubleshooting Your WAAS Network" chapter in the *Cisco Wide Area Application Services Configuration Guide*.

Viewing TCP Statistics

You can use the TCP Summary Report to view a summary of TCP optimization statistics for your WAAS system (from the System Dashboard) or for a specific device (from the Device Dashboard). Figure 1-5 on page 1-6 shows an example of the report.

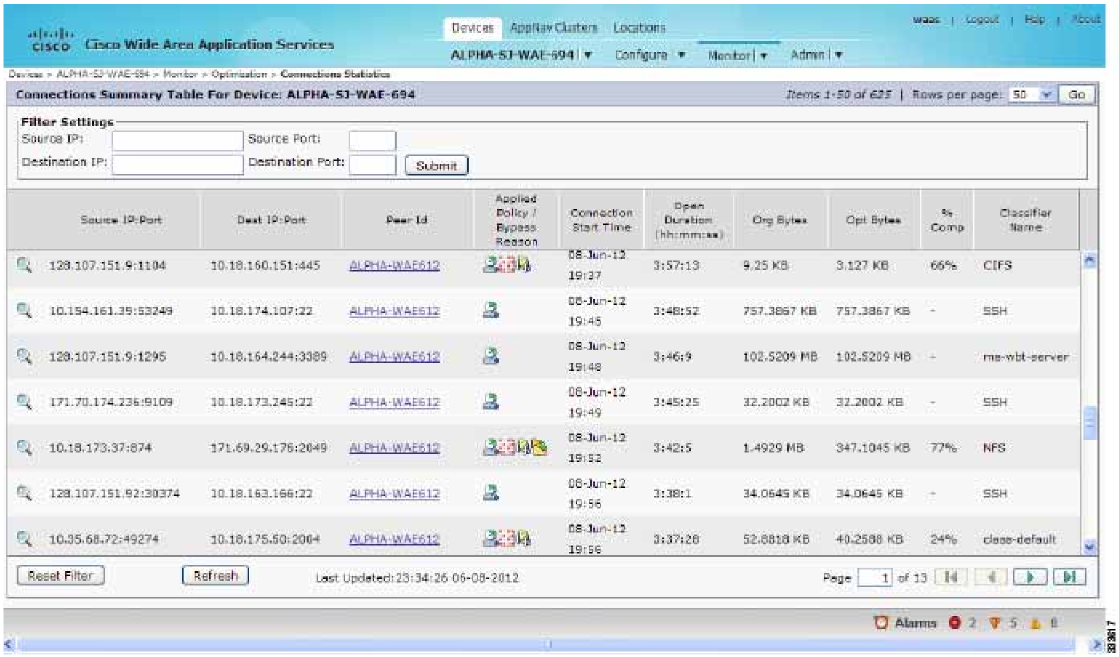
To display this report, choose **Monitor** > **Optimization** > **TCP Summary Report** from either dashboard. The report contains the following optimization charts:

- Traffic Summary
- Effective WAN Capacity
- Traffic Volume and Reduction
- Compression Summary
- Traffic Summary over Time
- Compression Summary over Time
- Network Traffic Summary

Viewing Connection Statistics

You can use the Connection Statistics Report to view all of the TCP connections handled by a device, as seen in Figure 1-8. To display this report, choose **Monitor** > **Optimization** > **Connection Statistics** in the Device Dashboard.

Figure 1-8 Connection Statistics Report


Cisco Wide Area Application Services
Devices
AppNav Clusters
Locations
ALPHA-SJ-WAE-694 ▾
Configure ▾
Monitor ▾
Admin ▾
waas | Logout | Help | About
Devices > ALPHA-SJ-WAE-694 > Monitor > Optimization > Connections Statistics
Go
Submit
Reset Filter
Refresh
Alarms 2 5 8
333617

Connections Summary Table For Device: ALPHA-SJ-WAE-694 *Items 1-50 of 625* | Rows per page: 50

Filter Settings
Source IP: Source Port:
Destination IP: Destination Port:

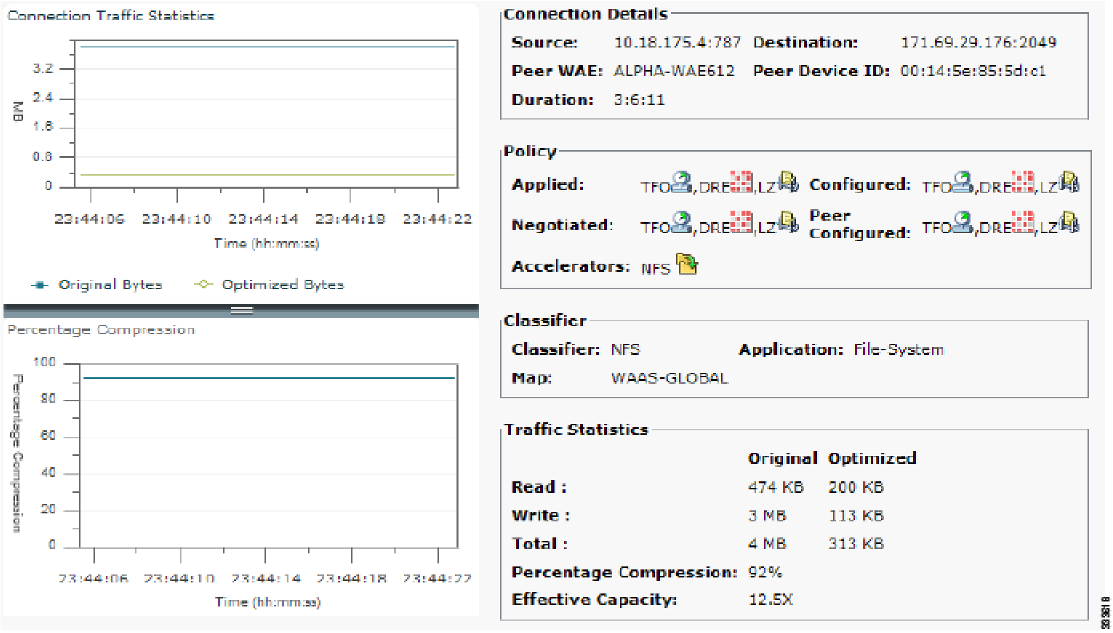
	Source IP:Port	Dest IP:Port	Peer Id	Applied Policy / Bypass Reason	Connection Start Time	Open Duration (hh:mm:ss)	Org Bytes	Opt Bytes	% Comp	Classifier Name
	128.107.151.9:1104	10.18.160.151:445	ALPHA-WAE612		08-Jun-12 19:37	3:57:13	9.25 KB	3.127 KB	66%	CIFS
	10.154.161.35:53249	10.18.174.107:22	ALPHA-WAE612		08-Jun-12 19:45	3:48:52	757.3867 KB	757.3867 KB	-	SSH
	128.107.151.9:1295	10.18.164.244:3389	ALPHA-WAE612		08-Jun-12 19:48	3:46:9	102.5209 MB	102.5209 MB	-	ms-wbt-server
	171.70.174.236:9109	10.18.173.245:22	ALPHA-WAE612		08-Jun-12 19:49	3:45:25	32.2002 KB	32.2002 KB	-	SSH
	10.18.173.37:874	171.69.29.176:2049	ALPHA-WAE612		08-Jun-12 19:52	3:42:5	1.4929 MB	347.1045 KB	77%	NFS
	128.107.151.92:30374	10.18.163.166:22	ALPHA-WAE612		08-Jun-12 19:56	3:38:1	34.0645 KB	34.0645 KB	-	SSH
	10.35.68.72:49274	10.18.175.50:2064	ALPHA-WAE612		08-Jun-12 19:56	3:37:28	52.8818 KB	40.2588 KB	24%	class-default

Last Updated: 23:34:26 06-08-2012 Page 1 of 13

The table lists all the active connections served by the selected WAE. The output provides key details about the flow by highlighting type of traffic, peer ID, percent compression, applied policies, and so forth.

To view additional connection details for a specific connection, click the magnifying glass icon to the left of the connection. The Connection Details Report appears, as shown in Figure 1-9.

Figure 1-9 Connection Details Report



Connection Details

Source: 10.18.175.4:787 **Destination:** 171.69.29.176:2049
Peer WAE: ALPHA-WAE612 **Peer Device ID:** 00:14:5e:85:5d:c1
Duration: 3:6:11

Policy

Applied: TFO, DRE, LZ **Configured:** TFO, DRE, LZ
Negotiated: TFO, DRE, LZ **Peer Configured:** TFO, DRE, LZ
Accelerators: NFS

Classifier

Classifier: NFS **Application:** File-System
Map: WAAS-GLOBAL

Traffic Statistics

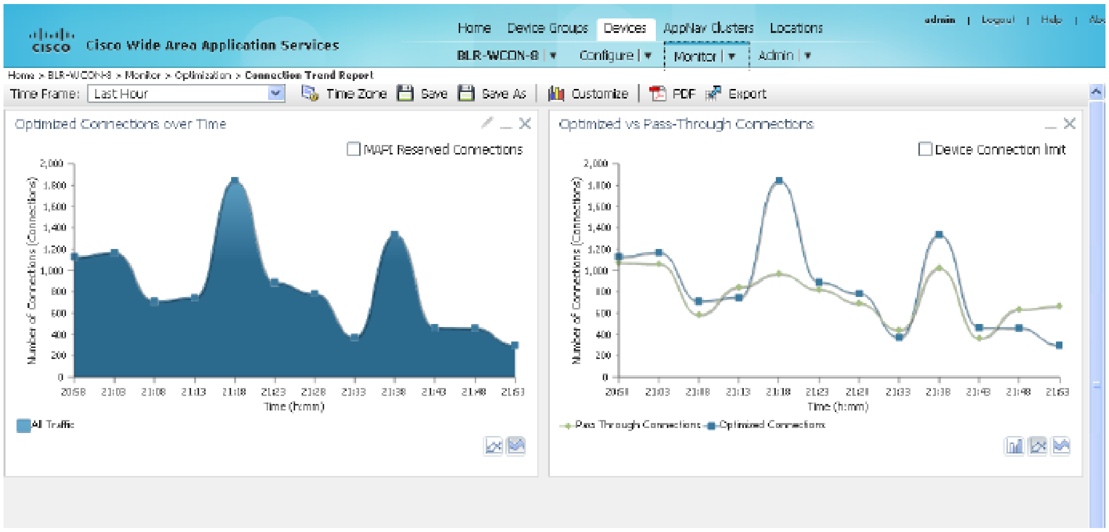
	Original	Optimized
Read :	474 KB	200 KB
Write :	3 MB	113 KB
Total :	4 MB	313 KB
Percentage Compression:	92%	
Effective Capacity:	12.5X	

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

Viewing Connection Trends

You can use the Connection Trend Report to view all of the traffic processed by a device, as seen in Figure 1-10. To display this report, choose **Monitor** > **Optimization** > **Connection Trend Report** in the Device Dashboard.

Figure 1-10 Connection Trend Report


Cisco Wide Area Application Services
Home
Device Groups
Devices
AppNav Clusters
Locations
admin | Logout | Help | Ab
BLR-WCON-8 | ▾
Configure | ▾
Monitor | ▾
Admin | ▾
Home > BLR-WCON-8 > Monitor > Optimization > Connection Trend Report
Time Zone
Save
Save As
Customize
PDF
Export
Optimized Connections over Time
□ MAPI Reserved Connections
Number of Connections (Connections)
2,000
1,800
1,600
1,400
1,200
1,000
800
600
400
200
0
20:58
21:03
21:08
21:13
21:18
21:23
21:28
21:33
21:38
21:43
21:48
21:53
Time (h:mm)
All Traffic
Optimized vs Pass-Through Connections
□ Device Connection limit
Number of Connections (Connections)
Time (h:mm)
Pass Through Connections
Optimized Connections

Time Frame: Last Hour

The Connection Trend Report provides data on the optimized and pass-through connections of all the traffic processed on the device. You can use this data to monitor the connection trends of all the applications on the device.

Viewing Acceleration Reports

The WAAS Central Manager GUI provides a number of statistical reports to help you monitor the performance boosts provided by different application accelerators.

This provides an example of one acceleration report:

- Viewing HTTPS Acceleration Statistics, page 1-12

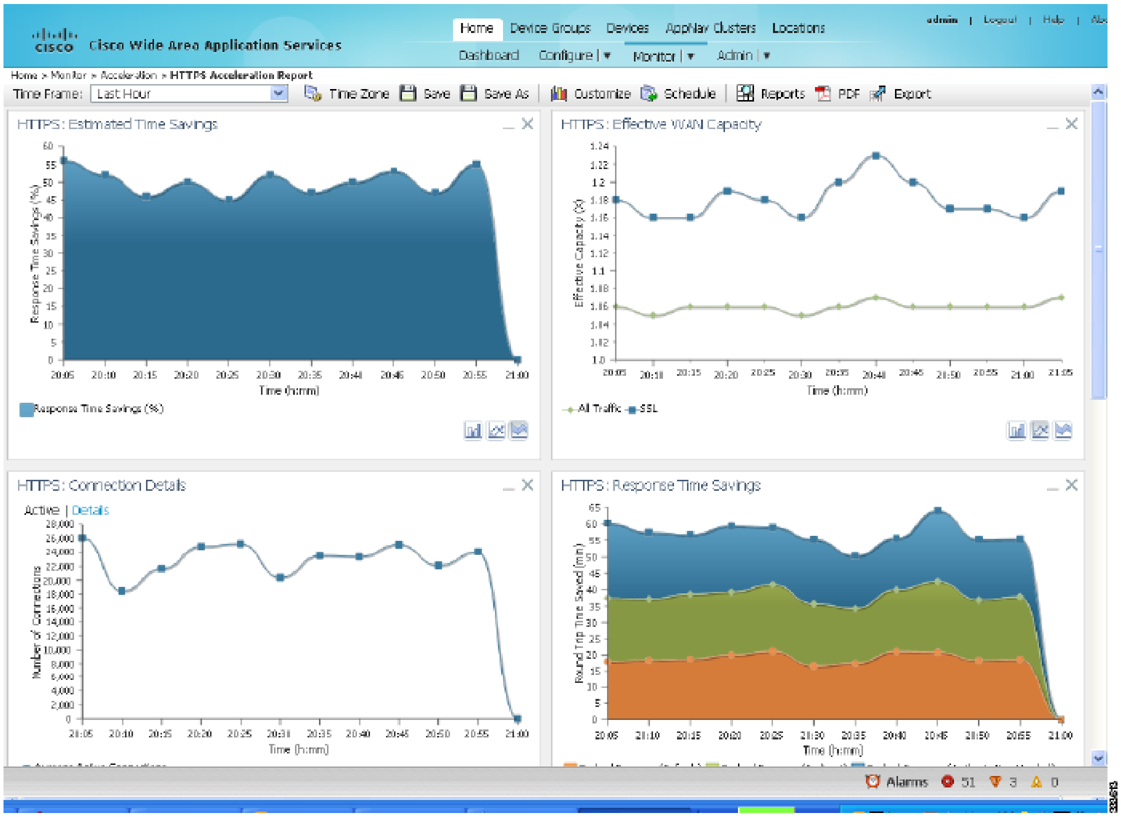
Similar reports are available for all of the available accelerators.

For more information, including a complete list of acceleration reports, see the "Monitoring and Troubleshooting Your WAAS Network" chapter in the *Cisco Wide Area Application Services Configuration Guide*.

Viewing HTTPS Acceleration Statistics

The HTTPS Acceleration Report, shown in Figure 1-11, displays details about HTTPS acceleration in your network (in the System Dashboard) or for a specific device (in the Device Dashboard). To view this report, choose **Monitor** > **Acceleration** > **HTTPS Acceleration Report** in either dashboard.

Figure 1-11 HTTPS Acceleration Report

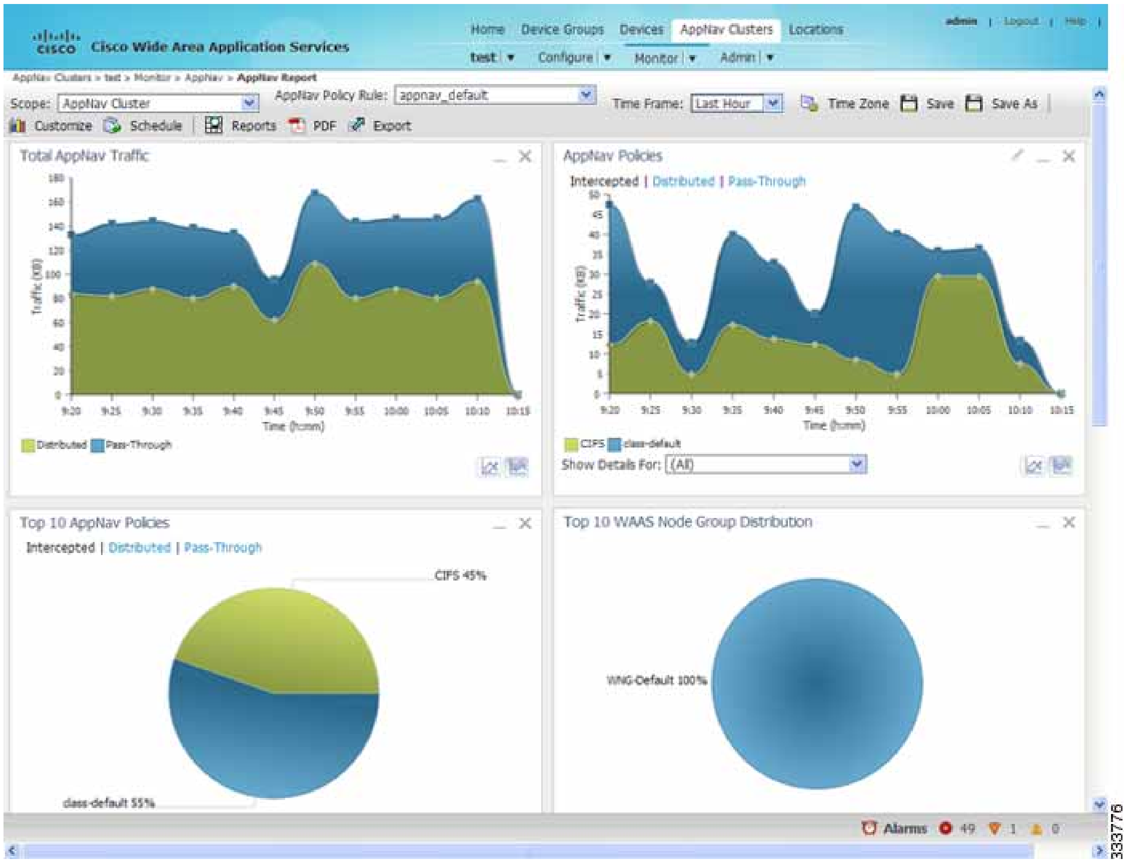


Viewing AppNav Reports

You can use the AppNav Report to monitor the status of an AppNav controller by choosing **Monitor** > **AppNav Report** from the Device Dashboard.

The AppNav Report shows a number of statistics about AppNav performance, as seen in Figure 1-12.

Figure 1-12 AppNav Report



Scope: AppNav Cluster

AppNav Policy Rule: appnav_default

Time Frame: Last Hour

Show Details For: (All)

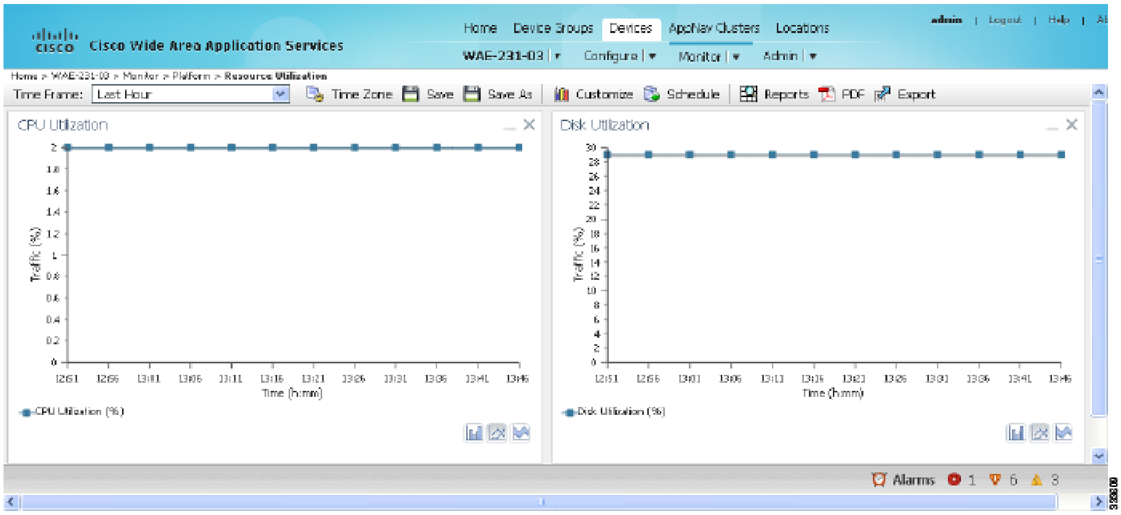
You can view information about intercepted and pass-through traffic, top AppNav policies, and the top reasons for AppNav distributing or passing data through.

Viewing Platform Reports

The platform reports allow you to monitor resource and utilization for your network. This section shows an example of one platform report: the Resource Utilization Report.

You can view resource utilization for a device by choosing **Monitor** > **Platform** > **Resource Utilization** in the Device Dashboard (see Figure 1-13).

Figure 1-13 Resource Utilization Report



The resource utilization report shows the percentage of CPU usage and disk utilization for the device.

Monitoring Logs and System Messages

The WAAS Central Manager logs information and messages about events and actions so you can track what has happened in your WAAS network. This section contains the following topics:

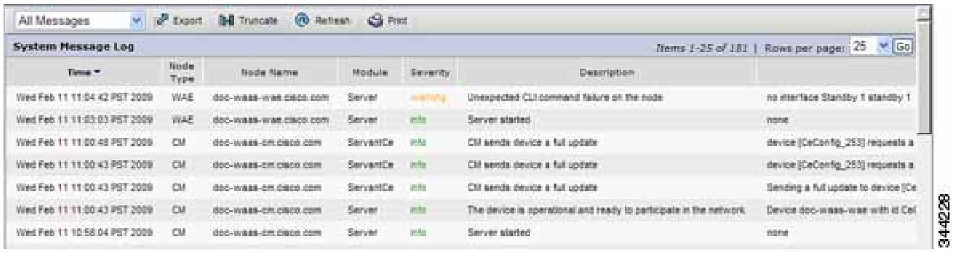
- Viewing the System Message Log, page 1-14
- Viewing the Audit Trail Log, page 1-15
- Viewing the Device Log, page 1-15

For more information, see the "Monitoring and Troubleshooting Your WAAS Network" chapter in the *Cisco Wide Area Application Services Configuration Guide*.

Viewing the System Message Log

You can use the system message log feature of the WAAS Central Manager GUI to view information about events that have occurred in your WAAS network. To view this log, an example of which is shown in Figure 1-14, choose **Admin > Logs > System Messages** in the System Dashboard.

Figure 1-14 System Message Log Window



System Message Log
Items 1-25 of 181 | Rows per page: 25 Go

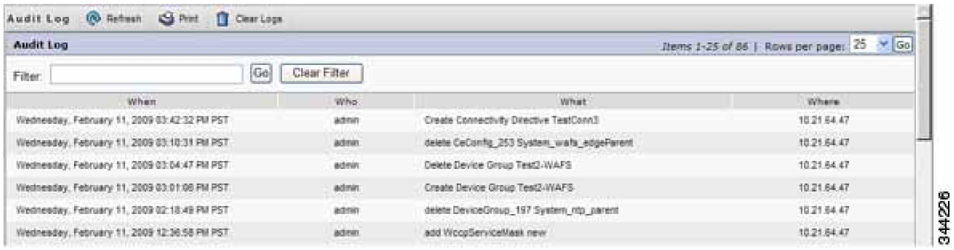
Time ▾	Node Type	Node Name	Module	Severity	Description	
Wed Feb 11 11:04:42 PST 2009	WAE	doc-waas-wae.cisco.com	Server	warning	Unexpected CLI command failure on the node	no interface Standby 1 standby 1
Wed Feb 11 11:03:03 PST 2009	WAE	doc-waas-wae.cisco.com	Server	info	Server started	none
Wed Feb 11 11:00:48 PST 2009	CM	doc-waas-cm.cisco.com	ServantCe	info	CM sends device a full update	device [CeConfig_253] requests a
Wed Feb 11 11:00:43 PST 2009	CM	doc-waas-cm.cisco.com	ServantCe	info	CM sends device a full update	device [CeConfig_253] requests a
Wed Feb 11 11:00:43 PST 2009	CM	doc-waas-cm.cisco.com	ServantCe	info	CM sends device a full update	Sending a full update to device [Ce
Wed Feb 11 11:00:43 PST 2009	CM	doc-waas-cm.cisco.com	Server	info	The device is operational and ready to participate in the network.	Device doc-waas-wae with id Cel
Wed Feb 11 10:58:04 PST 2009	CM	doc-waas-cm.cisco.com	Server	info	Server started	none

You can customize which messages are shown the log and how many lines to display in the log window.

Viewing the Audit Trail Log

Any time an activity changes the WAAS network, the Central Manager audits that user activity, storing the time and action taken into a log. You can view this audit trail (see Figure 1-15) by choosing **Admin** > **Logs** > **Audit Trail Log** in the System Dashboard.

Figure 1-15 Audit Trail Log Window



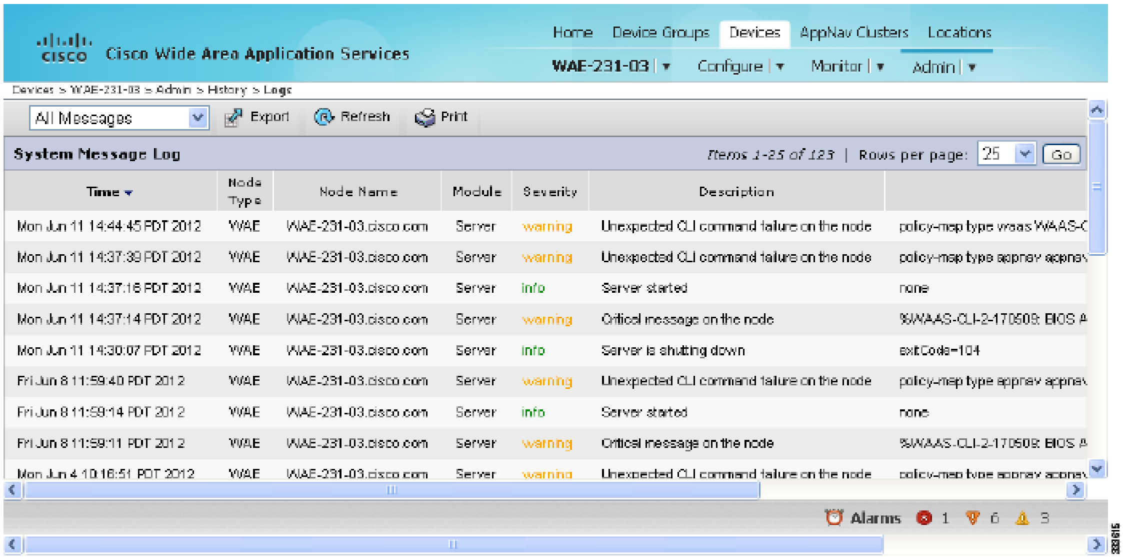
When	Who	What	Where
Wednesday, February 11, 2009 03:42:32 PM PST	admin	Create Connectivity Directive TestConn3	10.21.64.47
Wednesday, February 11, 2009 03:10:31 PM PST	admin	delete CeConfig_253 System_wafs_edgeParent	10.21.64.47
Wednesday, February 11, 2009 03:04:47 PM PST	admin	Delete Device Group Test2-WAFS	10.21.64.47
Wednesday, February 11, 2009 03:01:06 PM PST	admin	Create Device Group Test2-WAFS	10.21.64.47
Wednesday, February 11, 2009 02:18:49 PM PST	admin	delete DeviceGroup_197 System_ntp_parent	10.21.64.47
Wednesday, February 11, 2009 12:36:58 PM PST	admin	add WccpServiceMask new	10.21.64.47

Note that you can add filtering and select the number of rows to display in the log window.

Viewing the Device Log

You can view audit information for a specific device (see Figure 1-16) in your WAAS network by choosing **Admin** > **Logs** > **Device Logs** from the Device Dashboard window.

Figure 1-16 Device Log Window



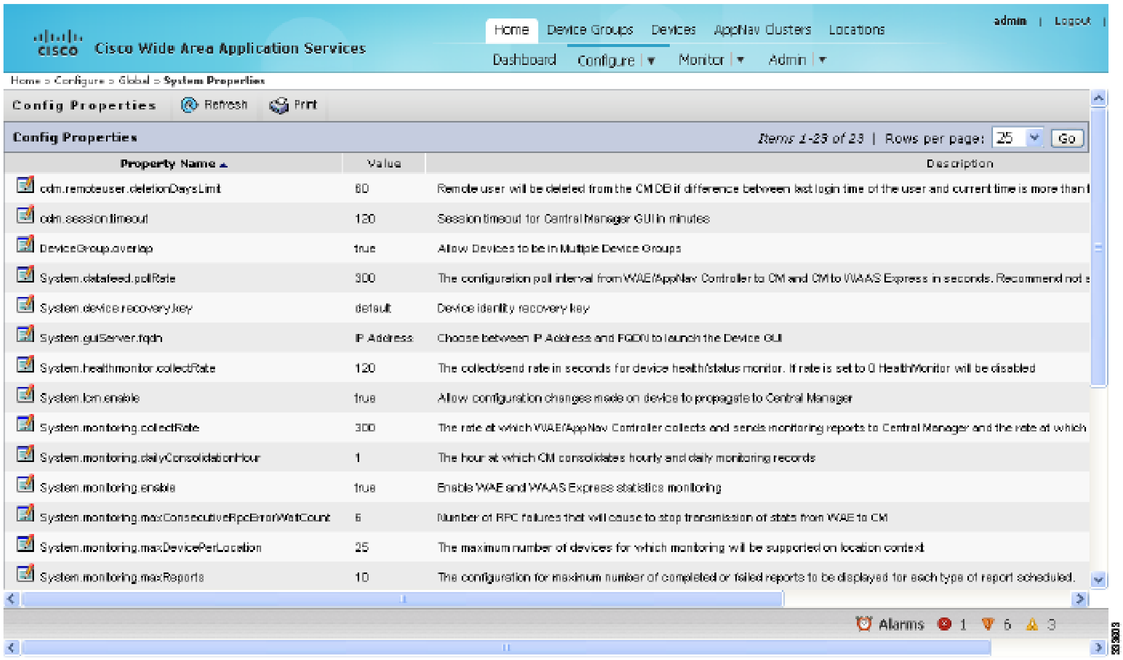
Time	Node Type	Node Name	Module	Severity	Description	
Mon Jun 11 14:44:45 PDT 2012	WAE	WAE-231-03.cisco.com	Server	warning	Unexpected CLI command failure on the node	policy-map type waas WAAS-C
Mon Jun 11 14:37:39 PDT 2012	WAE	WAE-231-03.cisco.com	Server	warning	Unexpected CLI command failure on the node	policy-map type appnav appnav
Mon Jun 11 14:37:16 PDT 2012	WAE	WAE-231-03.cisco.com	Server	info	Server started	none
Mon Jun 11 14:37:14 PDT 2012	WAE	WAE-231-03.cisco.com	Server	warning	Critical message on the node	%WAAS-CLI-2-170509: BIOS A
Mon Jun 11 14:30:07 PDT 2012	WAE	WAE-231-03.cisco.com	Server	info	Server is shutting down	exitCode=104
Fri Jun 8 11:59:40 PDT 2012	WAE	WAE-231-03.cisco.com	Server	warning	Unexpected CLI command failure on the node	policy-map type appnav appnav
Fri Jun 8 11:59:14 PDT 2012	WAE	WAE-231-03.cisco.com	Server	info	Server started	none
Fri Jun 8 11:59:11 PDT 2012	WAE	WAE-231-03.cisco.com	Server	warning	Critical message on the node	%WAAS-CLI-2-170509: BIOS A
Mon Jun 4 10:16:51 PDT 2012	WAE	WAE-231-03.cisco.com	Server	warning	Unexpected CLI command failure on the node	policy-map type appnav appnav

You can add filtering and select the number of rows to display in the log window. You can also export the log to a comma-separated values (csv) file.

Viewing System Properties

You can view and modify the current system properties by choosing **Configure > System Properties** from the System Dashboard. The Config Properties window appears (see Figure 1-17).

Figure 1-17 System Properties Window



Property Name ▲	Value	Description
cdm.remoteuser.deletionDaysLimit	60	Remote user will be deleted from the CMDB if difference between last login time of the user and current time is more than t
cdm.session.timeout	120	Session timeout for Central Manager GUI in minutes
DeviceGroup.overlap	true	Allow Devices to be in Multiple Device Groups
System.datafeed.pollRate	300	The configuration poll interval from WAE/AppNav Controller to CM and CM to WAAS Express in seconds. Recommend not s
System.device.recovery.key	default	Device identity recovery key
System.guiServer.fqdn	IP Address	Choose between IP Address and FQDN to launch the Device GUI
System.healthmonitor.collectRate	120	The collect/send rate in seconds for device health/status monitor. If rate is set to 0 HealthMonitor will be disabled
System.lcm.enable	true	Allow configuration changes made on device to propagate to Central Manager
System.monitoring.collectRate	300	The rate at which WAE/AppNav Controller collects and sends monitoring reports to Central Manager and the rate at which
System.monitoring.dailyConsolidationHour	1	The hour at which CM consolidates hourly and daily monitoring records
System.monitoring.enable	true	Enable WAE and WAAS Express statistics monitoring
System.monitoring.maxConsecutiveRpcErrorWaitCount	6	Number of RPC failures that will cause to stop transmission of stats from WAE to CM
System.monitoring.maxDevicePerLocation	25	The maximum number of devices for which monitoring will be supported on location context
System.monitoring.maxReports	10	The configuration for maximum number of completed or failed reports to be displayed for each type of report scheduled.

For more information, see the *Cisco Wide Area Application Services Configuration Guide* chapter on "Configuring Other System Settings."

Running CLI Commands from the WAAS Central Manager GUI

To run command-line interface (CLI) commands from the WAAS Central Manager GUI, first select a device in the dashboard, and then choose **Monitor > CLI Commands > Show Commands**.

The CLI includes numerous **show** commands, which are described in detail in the *Cisco Wide Area Application Services Command Reference*.

This section provides examples of several of the **show** commands, to give you an idea of the kind of information you can display. To access the **show** commands, follow these steps:

Step 1 Select a device in the dashboard.

Step 2 Choose **Monitor > CLI Commands > Show Commands**. The WAAS Show Commands window displays.

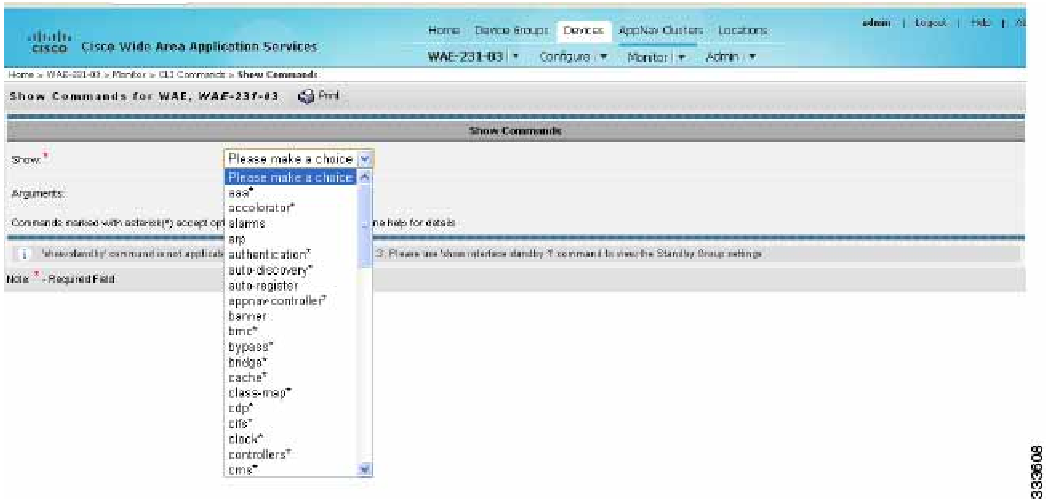
Step 3 Choose which command you want to run from the Show Commands dropdown list, as shown in Figure 1-18.

Step 4 Add any required or optional options for the command.

Step 5 Click **Submit**.

The command output displays in a popup window.

Figure 1-18 WAAS Show Commands



This section contains the following topics:

- show cms info Command, page 1-17
- show wccp status Command Output, page 1-18
- show wccp statistics Command Output, page 1-18
- show statistics connection Command Output, page 1-18
- show statistics connection optimized http Command Output, page 1-19
- show statistics dre Command Output, page 1-20
- show statistics tfo Command Output, page 1-20
- show interface GigabitEthernet Command Output, page 1-21
- show ip access-list Command Output, page 1-21

show cms info Command

The **show cms info** command output provides the WAE registration information with the last configuration synchronization time with WAAS Central Manager, which is useful when you suspect an application policy configuration issue.

```
WAE-231-03# show cms info
Device registration information :
Device Id                            = 3806
Device registered as                 = WAAS Appnav Controller
Current WAAS Central Manager         = 2.43.65.50
Registered with WAAS Central Manager = 2.43.65.50
Status                               = Online
Time of last config-sync             = Fri Jun  8 05:27:47 2012

CMS services information :
```

```
Service cms_ce is running
```

show wccp status Command Output

The **show wccp status** command output displays the current status of WCCP, including which services are enabled on the device.

```
WAE-231-03# show wccp status
WCCP Interception :
Configured State :  Enabled

Services Enabled on this WAE:
        TCP Promiscuous 61
        TCP Promiscuous 62
```

The **show wccp** command can be used with different options. For more information about using this command, see the *Cisco Wide Area Application Services Command Reference*.

show wccp statistics Command Output

The **show wccp statistics** command output includes three packets received counters, one of which should be incrementing to indicate that the WAE is receiving redirected packets.

```
WAE-231-03# show wccp statistics
Transparent GRE packets received:              0              <<< Packet received counters
Transparent non-GRE packets received:          212389542      <<<
Transparent non-GRE non-WCCP packets received: 0              <<<
Total packets accepted:                        158369766      <<<
Invalid packets received:                      0
Packets received with invalid service:         0
Packets received on a disabled service:        0
Packets received too small:                    0
Packets dropped due to zero TTL:               0
Packets dropped due to bad buckets:            42
Packets dropped due to no redirect address:    0
Packets dropped due to loopback redirect:      0
Pass-through pkts on non-owned bucket:         0
Connections bypassed due to load:              0               <<< Bypass counter
Packets sent back to router:                   3
GRE packets sent to router (not bypass):       0
Packets sent to another WAE:                   0
...
```

If the device is under heavy load and no new flows can be optimized, the Connections bypassed due to load counter increments. A nonzero value for this counter indicates that the device is under overload or has previously gone into overload and should be further investigated.

show statistics connection Command Output

The **show statistics connection** command output displays all connection statistics for a WAAS device.

```
sjc22-00a-WAE-674# show statistics connection

Current Active Optimized Flows:                      7
   Current Active Optimized TCP Plus Flows:          2
   Current Active Optimized TCP Only Flows:          12
   Current Active Optimized TCP Preposition Flows:   0
Current Active Auto-Discovery Flows:                 16
Current Reserved Flows:                              40
Current Active Pass-Through Flows:                   25
Historical Flows:                                    597


D:DRE,L:LZ,T:TCP Optimization RR:Total Reduction Ratio
A:AOIM,C:CIFS,E:EPM,G:GENERIC,H:HTTP,I:ICA,M:MAPI,N:NFS,S:SSL,W:WAN SECURE,V:VID
EO
X: SMB Signed Connection

ConnID       Source IP:Port          Dest IP:Port            PeerID Accel RR
445095   10.34.209.79:54455     199.47.216.147:80 58:8d:09:d1:bc:c1 THDL  87.1%
447076  10.34.209.123:50028   171.70.151.151:1344 58:8d:09:d1:bc:c1 TG    00.0%
447268  10.34.209.106:56632     171.71.160.68:445 58:8d:09:d1:bc:c1 TCDL  07.9%
447293  10.34.209.123:63628      172.25.210.42:22 58:8d:09:d1:bc:c1 T     00.0%
447296  10.34.209.106:62564 128.107.191.124:12834 58:8d:09:d1:bc:c1 TG    00.0%
447349   10.34.215.74:31787    10.32.176.206:7878 00:21:5e:76:1d:64 TL    04.8%
447350  10.34.209.106:64183 128.107.191.124:12834 58:8d:09:d1:bc:c1 TG    00.0%
...
```

The **show statistics** command can be used with different options. For more information about using this command, see the *Cisco Wide Area Application Services Command Reference*.

show statistics connection optimized http Command Output

The **show statistics connection optimized http** command output displays the connection optimized by the http application accelerator.

```
sjc22-00a-WAE-674# show statistics connection optimized http

Current Active Optimized Flows:                      14
   Current Active Optimized TCP Plus Flows:          2
   Current Active Optimized TCP Only Flows:          11
   Current Active Optimized TCP Preposition Flows:   0
Current Active Auto-Discovery Flows:                 16
Current Reserved Flows:                              40
Current Active Pass-Through Flows:                   27
Historical Flows:                                    593


D:DRE,L:LZ,T:TCP Optimization RR:Total Reduction Ratio
A:AOIM,C:CIFS,E:EPM,G:GENERIC,H:HTTP,I:ICA,M:MAPI,N:NFS,S:SSL,W:WAN SECURE,V:VID
EO
X: SMB Signed Connection

ConnID       Source IP:Port          Dest IP:Port            PeerID Accel RR
445095   10.34.209.79:54455     199.47.216.147:80 58:8d:09:d1:bc:c1 THDL  87.2%
```

The **show statistics connection optimized** command can be used with different options. For more information about using this command, see the *Cisco Wide Area Application Services Command Reference*.

show statistics dre Command Output

The **show statistics dre** command output displays overall Data Redundancy Eliminate (DRE) statistics. The command output includes compression ratios for both encode and decode and details about DRE age, cache size available, and used percentage.

```
sjc22-00a-WAE-674# show statistics dre

Cache:
    Status: Usable, Oldest Data (age): 739d
    Total usable disk size: 311289 MB,  Used: 35.12%                             <<< Cache

Connections:   Total (cumulative): 428069   Active: 18

Encode:
   Overall: msg:    8879839, in:  36648 MB, out:  19474 MB, ratio:  46.86%      <<< Encode
       DRE: msg:    8294549, in:  36366 MB, out:  21154 MB, ratio:  41.83%
DRE Bypass: msg:    6273500, in:    278 MB
        LZ: msg:    6917737, in:  10361 MB, out:   8365 MB, ratio:  19.26%      <<< LZ
 LZ Bypass: msg:    1962102, in:  11071 MB
    Avg latency:      0.335 ms, Avg msg size:   4327 B
  Message size distribution:
    0-1K=18%  1K-5K=65%  5K-15K=7%  15K-25K=4%  25K-40K=3%  >40K=1%
Decode:
   Overall: msg:    2677837, in:    615 MB, out:   2931 MB, ratio:  79.00%      <<< Decode
       DRE: msg:    1511198, in:    648 MB, out:   2296 MB, ratio:  71.75%
DRE Bypass: msg:    2346105, in:    635 MB
        LZ: msg:    1254878, in:    401 MB, out:   1089 MB, ratio:  63.15%      <<< LZ
 LZ Bypass: msg:    1422959, in:    214 MB
    Avg latency:      0.059 ms, Avg msg size:   1148 B
  Message size distribution:
    0-1K=85%  1K-5K=9%  5K-15K=1%  15K-25K=1%  25K-40K=2%  >40K=0%
```

The **show statistics dre** command can be used with the **detail option** to show more detailed information.

show statistics tfo Command Output

The **show statistics tfo** command output displays Traffic Flow Optimization (TFO) statistics for a WAE.

```
sjc22-00a-WAE-674# show statistics tfo
  Total number of connections                          : 428073
  No. of active connections                            : 21
  No. of pending (to be accepted) connections          : 0
  No. of bypass connections                            : 135585
  No. of normal closed conns                           : 301317
  No. of reset connections                             : 126735
     Socket write failure                              : 1060
     Socket read failure                               : 0
     WAN socket close while waiting to write           : 285
     AO socket close while waiting to write            : 205
     WAN socket error close while waiting to read      : 0
     AO socket error close while waiting to read       : 6435
     DRE decode failure                                : 0
     DRE encode failure                                : 0
     Connection init failure                           : 0
     WAN socket unexpected close while waiting to read : 57305
     Exceeded maximum number of supported connections  : 0
     Buffer allocation or manipulation failed          : 0
     Peer received reset from end host                 : 59283
     DRE connection state out of sync                  : 0
     Memory allocation failed for buffer heads         : 0
     Unoptimized packet received on optimized side     : 2162
...
```

The **show statistics tfo** command can be used with different options. For more information about using this command, see the *Cisco Wide Area Application Services Command Reference*.

show interface GigabitEthernet Command Output

The **show interface GigabitEthernet** command displays GigabitEthernet interface device information. A speed and duplex mismatch is one of the most common reasons for poor performance.

```
WAE-231-03# show interface GigabitEthernet 1/0
Description this is my interception interface
lsp: Link State Propagation
flow sync: AppNav Controller is in the process of flow sync
Ethernet Address                    : 50:3d:e5:9d:ea:79
Internet Address                    : --
Netmask                             : --
Admin State                         : Down
Operation State                     : Down
Maximum Transfer Unit Size          : 1500
Input Errors                        : 0
Input Packets Dropped               : 0
Packets Received                    : 0
Output Errors                       : 0
Output Packets Dropped              : 0
Load Interval                       : 30
Input Throughput                    : 0 bits/sec, 0 packets/sec
Output Throughput                   : 0 bits/sec, 0 packets/sec
Packets Sent                        : 0
Auto-negotiation                    : On                     <<< Auto-negotiate status
Full Duplex                         : Yes                    <<< Full duplex status
Speed                               : 1000 Mbps              <<< Speed

Interception Statistics
  Input Packets Forwarded/Bridged   : 0
  Input Packets Redirected          : 0
  Input Packets Punted              : 0
  Input Packets Dropped             : 0
  Output Packets Forwarded/Bridged  : 0
  Output Packets Injected           : 0
  Output Packets Dropped            : 0
```

The **show interface** command can be used with different options. For more information about using this command, see the *Cisco Wide Area Application Services Command Reference*.

show ip access-list Command Output

The **show ip access-list** command displays the access lists that are defined and applied to specific interfaces or appliances on a WAAS device.

```
WAE-231-03# show ip access-list
Space available:
    49 access lists
   499 access list conditions
 32619 TCAM Entries

Standard IP access list myacl
   1 permit 192.168.1.0 0.0.0.255
```

```
     (implicit deny any: 0 matches, SN=0, ANC=0)
   total invocations: 0 (SN=0, ANC=0)
    [Legend: SN = Service Node ACL Hits, ANC = AppNav Controller ACL Hits]

Interface access list references:
  None Configured

Application access list references:
  No applications registered.
```

CHAPTER 2

Monitoring Traffic Interception

This chapter describes how to use traffic interception to monitor your WAAS devices and contains the following sections:

- Verifying WCCPv2 Interception, page 2-1
- Verifying Inline Interception, page 2-7

Verifying WCCPv2 Interception

This section describes several Cisco IOS and WAAS WCCP commands that are available to verify if WCCP interception is working correctly.

This section contains the following topics:

- show ip wccp IOS Command Output, page 2-1
- show wccp WAAS Command Outputs, page 2-6

show ip wccp IOS Command Output

The **show ip wccp** IOS command output provides an WCCP inventory that includes the number of routers, WAEs or service group, packets redirected, and forwarding and return method. This command is most commonly used to verify if WCCP interception is working correctly.

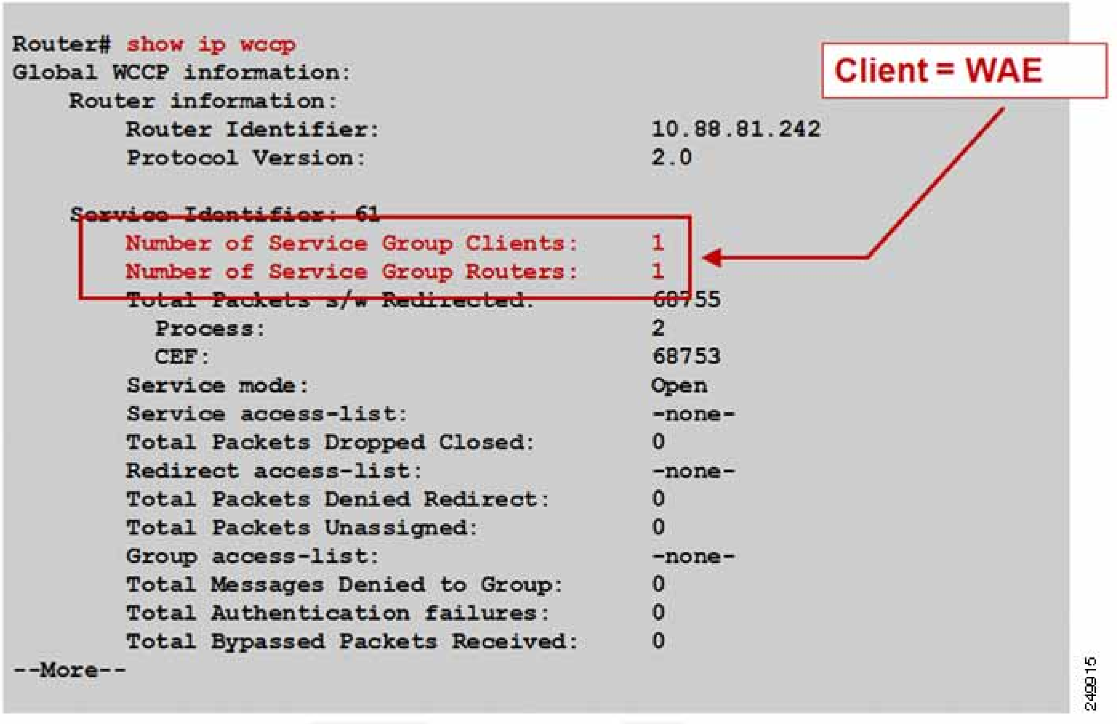
The command syntax is as follows:

show ip wccp [*service_group#*] [**detail**]

The following examples show how to use the command both with and without the optional argument and keyword.

Figure 2-1 highlights the area of the **show ip wccp** IOS command output that show that there is one intercepting router and one WAE registered to Service Group 61.

Figure 2-1 Command Output Sample 1: show ip wccp

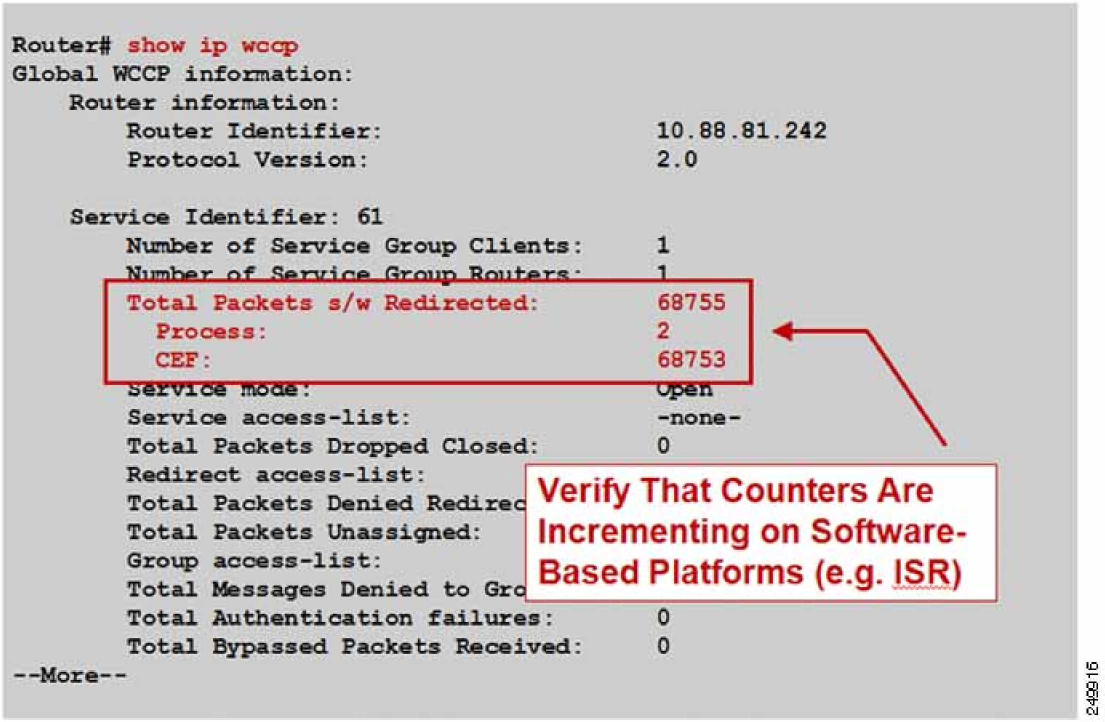


```
Router# show ip wccp
Global WCCP information:
    Router information:
        Router Identifier:                      10.88.81.242
        Protocol Version:                       2.0

    Service Identifier: 61
        Number of Service Group Clients:        1
        Number of Service Group Routers:        1
        Total Packets s/w Redirected:           68755
          Process:                              2
          CEF:                                  68753
        Service mode:                           Open
        Service access-list:                    -none-
        Total Packets Dropped Closed:           0
        Redirect access-list:                   -none-
        Total Packets Denied Redirect:          0
        Total Packets Unassigned:               0
        Group access-list:                      -none-
        Total Messages Denied to Group:         0
        Total Authentication failures:          0
        Total Bypassed Packets Received:        0
--More--
```

Figure 2-2 highlights the area of the **show ip wccp** IOS command output that shows that the Total Packets s/w Redirect counter is incrementing on software-based platforms (for example, Cisco ISR).

Figure 2-2 Command Output Sample 2: show ip wccp



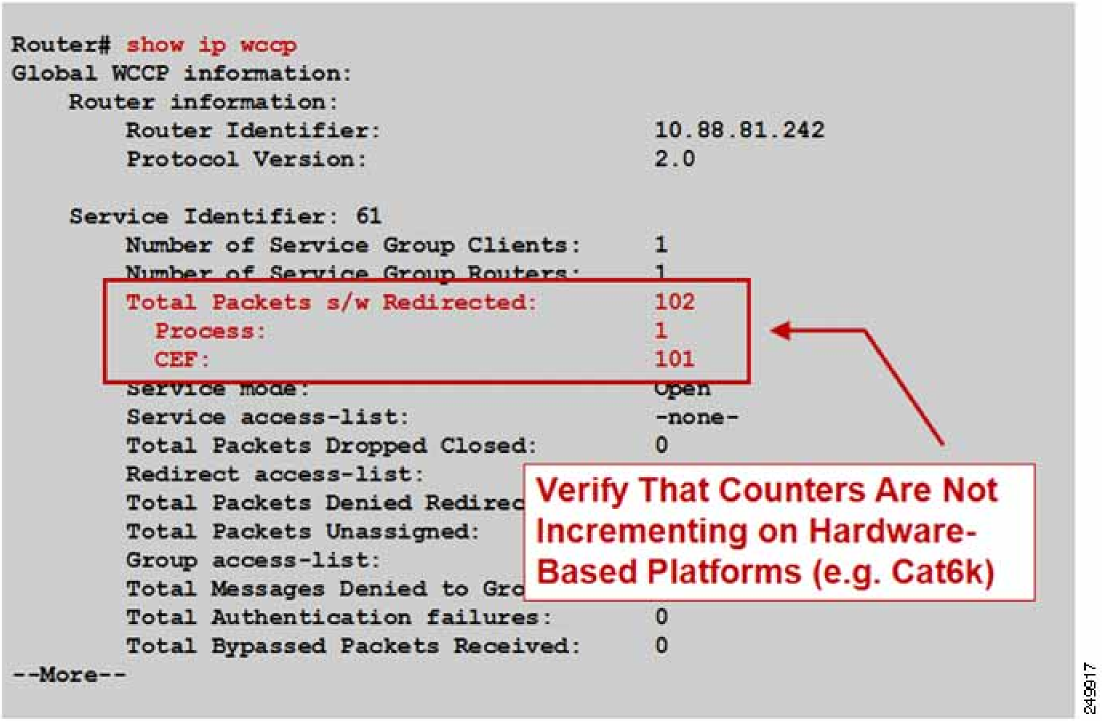
```
Router# show ip wccp
Global WCCP information:
    Router information:
        Router Identifier:                    10.88.81.242
        Protocol Version:                     2.0

    Service Identifier: 61
        Number of Service Group Clients:      1
        Number of Service Group Routers:      1
        Total Packets s/w Redirected:         68755
          Process:                            2
          CEF:                                68753
        Service mode:                         Open
        Service access-list:                  -none-
        Total Packets Dropped Closed:         0
        Redirect access-list:
        Total Packets Denied Redirec
        Total Packets Unassigned:
        Group access-list:
        Total Messages Denied to Gro
        Total Authentication failures:        0
        Total Bypassed Packets Received:      0
--More--
```

Verify That Counters Are Incrementing on Software-Based Platforms (e.g. ISR)

Figure 2-3 highlights the area of the **show ip wccp** IOS command output that shows that the Total Packets s/w Redirect counter is not incrementing on hardware-based platforms (for example, Cisco Catalyst 6500 Series Switches).

Figure 2-3   Command Output Sample 3: show ip wccp



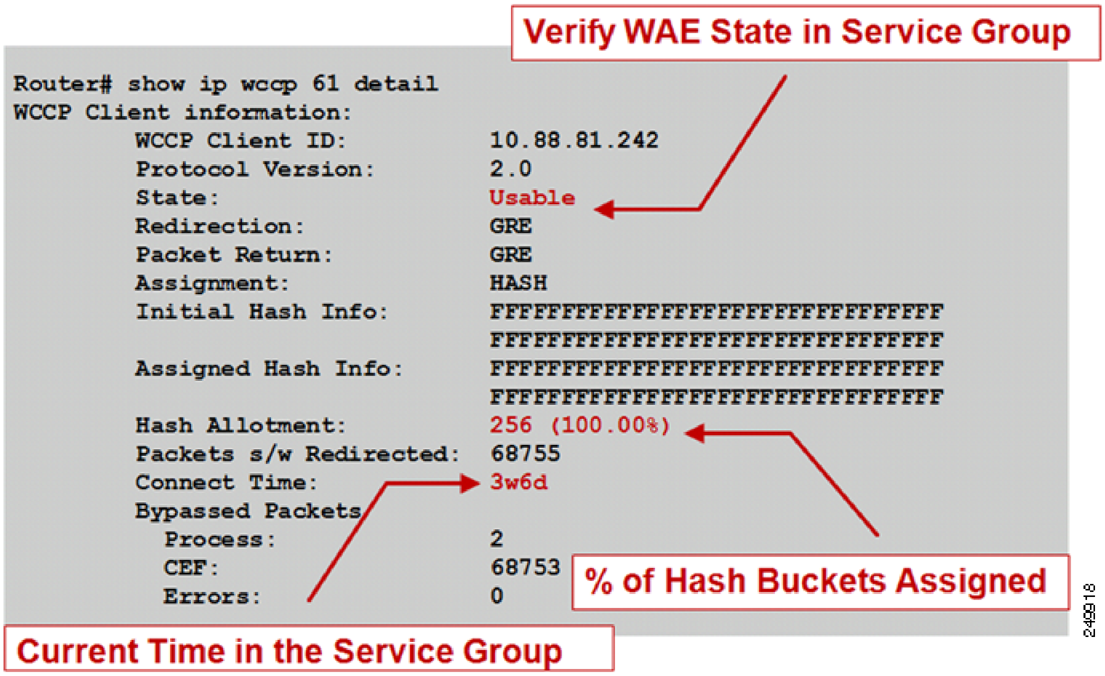
```
Router# show ip wccp
Global WCCP information:
    Router information:
        Router Identifier:                     10.88.81.242
        Protocol Version:                      2.0

    Service Identifier: 61
        Number of Service Group Clients:       1
        Number of Service Group Routers:       1
        Total Packets s/w Redirected:          102
          Process:                             1
          CEF:                                 101
        Service mode:                          Open
        Service access-list:                   -none-
        Total Packets Dropped Closed:          0
        Redirect access-list:
        Total Packets Denied Redirec
        Total Packets Unassigned:
        Group access-list:
        Total Messages Denied to Gro
        Total Authentication failures:         0
        Total Bypassed Packets Received:       0
--More--
```

Verify That Counters Are Not Incrementing on Hardware-Based Platforms (e.g. Cat6k)

The **show ip wccp** *service_group#* **detail** IOS command output provides information about the state, redirection and return methods used, connect time, and so forth. Figure 2-4 shows an example output from a software-based platform where the default redirection and assignment methods are used.

Figure 2-4 Command Output Sample 1: show ip wccp service_group# detail



Verify WAE State in Service Group

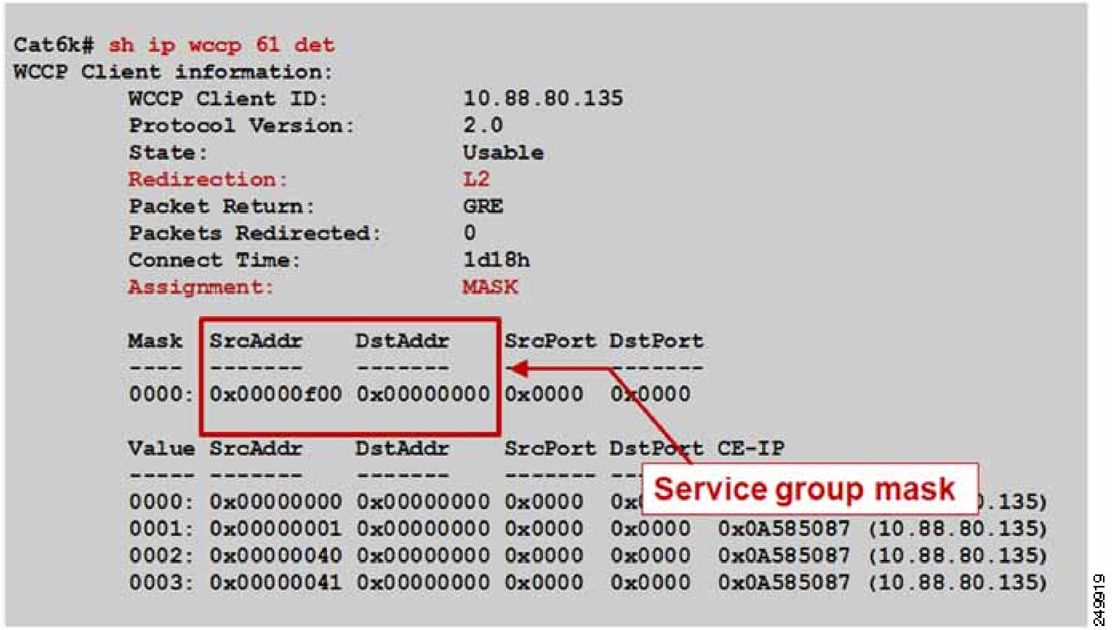
```
Router# show ip wccp 61 detail
WCCP Client information:
        WCCP Client ID:          10.88.81.242
        Protocol Version:        2.0
        State:                   Usable
        Redirection:             GRE
        Packet Return:           GRE
        Assignment:              HASH
        Initial Hash Info:       FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF
                                 FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF
        Assigned Hash Info:      FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF
                                 FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF
        Hash Allotment:          256 (100.00%)
        Packets s/w Redirected:  68755
        Connect Time:            3w6d
        Bypassed Packets
          Process:               2
          CEF:                   68753
          Errors:                0
```

% of Hash Buckets Assigned

Current Time in the Service Group

Figure 2-5 shows an example output from a hardware-based platform that is configured for Layer 2 redirect and mask assignment. The CLI output is slightly different, reflecting these configured parameters.

Figure 2-5 Command Output Sample 2: show ip wccp service_group# detail



```
Cat6k# sh ip wccp 61 det
WCCP Client information:
        WCCP Client ID:          10.88.80.135
        Protocol Version:        2.0
        State:                   Usable
        Redirection:             L2
        Packet Return:           GRE
        Packets Redirected:      0
        Connect Time:            1d18h
        Assignment:              MASK

        Mask  SrcAddr    DstAddr    SrcPort DstPort
        ----  --------   --------   ------- -------
        0000: 0x00000f00 0x00000000 0x0000  0x0000

        Value SrcAddr    DstAddr    SrcPort DstPort CE-IP
        ----- --------   --------   ------- --
        0000: 0x00000000 0x00000000 0x0000  0x                         .135)
        0001: 0x00000001 0x00000000 0x0000  0x0000  0x0A585087 (10.88.80.135)
        0002: 0x00000040 0x00000000 0x0000  0x0000  0x0A585087 (10.88.80.135)
        0003: 0x00000041 0x00000000 0x0000  0x0000  0x0A585087 (10.88.80.135)
```

Service group mask

show wccp WAAS Command Outputs

You can use the **show wccp** WAAS commands that are available from the WAE CLI to verify that WCCP is configured and operating properly.

This section contains the following topics:

- show wccp services Command Output, page 2-6
- show wccp status Command Output, page 2-6
- show wccp routers Command Output, page 2-6
- show wccp statistics Command Output, page 2-7

show wccp services Command Output

You can use the **show wccp services** command to display which WCCP services are configured.

```
WAE# show wccp services

Services Enabled on this WAE:
        TCP Promiscuous 61
        TCP Promiscuous 62
```

show wccp status Command Output

The **show wccp status** command displays the enabled state of WCCP and the configured service IDs.

```
WAE# show wccp status
WCCP Interception :
Configured State :  Enabled

Services Enabled on this WAE:
        TCP Promiscuous 61
        TCP Promiscuous 62
```

show wccp routers Command Output

The **show wccp routers** command displays information about the routers seen and not seen by the WAE.

```
WAE# show wccp routers
Router Information for Service Id: 61
        Routers Seeing this Wide Area Engine(1)
        Router Id       Sent To
        10.43.228.165    10.43.228.65
        Routers not Seeing this Wide Area Engine
        10.10.10.45    -Redirect Method Mismatch-
        Routers Notified of from other WAE's
                -NONE-

Router Information for Service Id: 62
        Routers Seeing this Wide Area Engine(1)
        Router Id       Sent To
        10.43.228.165    10.43.228.65
        Routers not Seeing this Wide Area Engine
        10.10.10.45    -Redirect Method Mismatch
        Routers Notified of from other WAE's
                -None-
```

show wccp statistics Command Output

The **show wccp statistics** displays WCCP generic routing encapsulation packet-related information. You know that WCCP redirection is working if either of the first two lines of output is incrementing:

```
WAE# show wccp statistics
Transparent GRE packets received:             0
Transparent non-GRE packets received:         212389542
Transparent non-GRE non-WCCP packets received: 0
Total packets accepted:                       158369766
Invalid packets received:                     0
Packets received with invalid service:        0
Packets received on a disabled service:       0
Packets received too small:                   0
...
```

Verifying Inline Interception

This section describes how to use the **show interface** command to verify inline interception configuration and proper operation.

This section contains the following topics:

- show interface inlineGroup Command Output, page 2-7
- show interface InlinePort Command Output, page 2-7

show interface inlineGroup Command Output

You can use the **show interface InlineGroup** command to display the inline group information and the slot and inline group number for the selected interface.

```
WAE612# show interface InlineGroup 1/0
Interface is in intercept operating mode.
Standard NIC mode is off.
Disable bypass mode is off.
VLAN IDs configured for inline interception: All
Watchdog timer is enabled.
Timer frequency: 1600 ms.
Autoreset frequency 500 ms.
The watchdog timer will expire in 1221 ms.
```

The inline interface operates in two modes:

- Intercept operating mode—Packets are passed to WAAS for potential optimization.
- Bypass operating mode—Mechanical bypass between ports in InlineGroup during a failure or administrative shutdown (not applicable on Cisco AppNav Controller Interface Modules).

show interface InlinePort Command Output

You can use the **show interface InlinePort** command to display the inline port information for the selected interface.

```
WAE# show interface InlinePort 1/0 lan
```

```
Ethernet Address                    : 50:3d:e5:9c:8f:45
Internet Address                    : --
Netmask                             : --
Admin State                         : Up
Operation State                     : Running
Maximum Transfer Unit Size          : 1500
Input Errors                        : 0
Input Packets Dropped               : 0
Packets Received                    : 4074292
Output Errors                       : 0
Output Packets Dropped              : 0
Load Interval                       : 30
Input Throughput                    : 12538 bits/sec, 13 packets/sec
Output Throughput                   : 23235 bits/sec, 11 packets/sec
Packets Sent                        : 3334662
Auto-negotiation                    : On
Full Duplex                         : Yes
Speed                               : 1000 Mbps
```

For more information about troubleshooting WCCP, see the *WAAS Troubleshooting Guide* available on Cisco DocWiki.

CHAPTER 3

Monitoring WAAS Using SNMP

This chapter describes how to use the Simple Network Management Protocol (SNMP) to monitor your WAAS devices. SNMP is an interoperable standards-based protocol that allows for external monitoring of WAAS devices through an SNMP agent.

For more information about using and configuring SNMP, see the "Configuring SNMP Monitoring" chapter in the *Cisco Wide Area Application Services Configuration Guide*.

This chapter contains the following sections:

Information About Supported MIBs

This section describes the Cisco-specific MIBs that are supported by WAAS as shown in Table 3-1.

Table 3-1 MIBs Supported by WAAS

MIB	Description
CISCO-APPNAV-MIB	Provides information about AppNav objects, including WAAS nodes, WAAS node groups, AppNav controllers, and AppNav controller groups.
CISCO-CONTENT-ENGINE-MIB	The MIB module for the Cisco WAAS device from Cisco Systems. The following objects from this MIB are supported: • cceAlarmCriticalCount • cceAlarmMajorCount • cceAlarmMinorCount • cceAlarmHistTableSize
CISCO-ENTITY-ASSET-MIB	Monitors the asset information of items in the ENTITY-MIB (RFC 2037) entPhysicalTable. This MIB lists the orderable part number, serial number, hardware revision, manufacturing assembly number and revision, firmware ID and revision (if any) and software ID and revision (if any) of relevant entities listed in ENTITY-MIB entPhysicalTable.

Table 3-1 MIBs Supported by WAAS (continued)

MIB	Description
CISCO-SMI	The MIB module for Cisco Enterprise Structure of Management Information. There is nothing to query in this MIB; it describes the structure of Cisco MIBs.
CISCO-WAN-OPTIMIZATION-MIB	Provides the following information: • application optimizer status and statistics • TFO statistics • application, policy map, and class map statistics
ENTITY-MIB	Represents multiple logical entities supported by a single SNMP agent. The entConfigChange notification is supported. This MIB is documented in RFC 2737.
EVENT-MIB	Defines event triggers and actions for network management purposes. The MIB is published as RFC 2981.
HOST-RESOURCES-MIB	Manages host systems. The term “host” implies any computer that communicates with other similar computers connected to the Internet. The HOST-RESOURCES-MIB does not necessarily apply to devices whose primary function is communications services (terminal servers, routers, bridges, monitoring equipment). This MIB provides attributes that are common to all Internet hosts, for example, personal computers and systems that run variants of UNIX.
IF-MIB	Supports querying for interface-related statistics including 64-bit interface counters. These counters include received and sent octets, unicast, multicast, and broadcast packets on the device interfaces. All the objects from ifXEntry are supported except for ifCounterDiscontinuityTime. This MIB is documented in RFC 2233.
MIB-II	The Internet Standard MIB that is documented in RFC 1213 and for use with network management protocols in TCP/IP-based Internets. This MIB is found in the RFC1213-MIB file in the v1 directory on the download site (other MIBs are in the v2 directory).
SNMP-COMMUNITY-MIB	Documented in RFC 2576.
SNMP-FRAMEWORK-MIB	Documented in RFC 2571.
SNMP-NOTIFICATION-MIB	Documented in RFC 3413.
SNMP-TARGET-MIB	Documented in RFC 3413.
SNMP-USM-MIB	Documented in RFC 2574.
SNMPv2-MIB	Documented in RFC 1907. This MIB supports the following notifications: • coldStart • linkUp • linkDown • authenticationFailure
SNMP-VACM-MIB	Documented in RFC 2575.

Downloading Supported MIBs

All supported MIB files can be downloaded from the following Cisco FTP locations:

- ftp://ftp.cisco.com/pub/mibs/v2
- ftp://ftp.cisco.com/pub/mibs/v1

The MIB objects that are defined in each MIB are described in the MIB files and are self-explanatory.

Working with SNMP Traps

This section contains the following topics:

- Enabling SNMP Traps, page 3-3
- Viewing SNMP Trigger Lists, page 3-4
- Defining New Traps, page 3-5

Enabling SNMP Traps

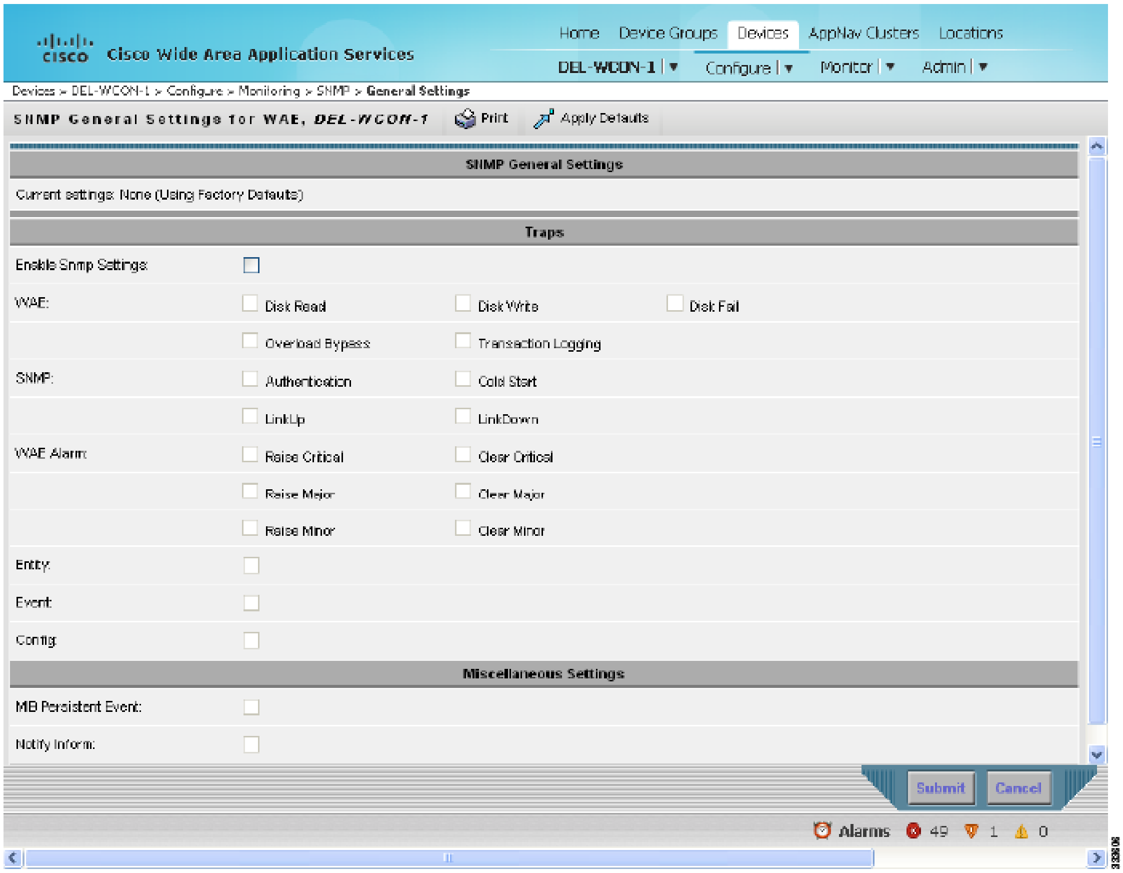
To send SNMP traps, follow these steps:

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

Step 2 Choose **Configure** > **Monitoring** > **SNMP** > **General Settings**. The SNMP General Settings window appears. See Figure 3-1. The settings window display which traps are enabled for the device or group.

Step 3 Configure the trap settings as desired. For more information, see the "Configuring SNMP Monitoring" chapter in the *Cisco Wide Area Application Services Configuration Guide*.

Figure 3-1 SNMP General Settings Window



SNMP General Settings for WAE, *DEL-WCON-1*

SNMP General Settings

Current settings: None (Using Factory Defaults)

Traps

Enable Snmp Settings:	□		
WAE:	□ Disk Read	□ Disk Write	□ Disk Fail
	□ Overload Bypass	□ Transaction Logging	
SNMP:	□ Authentication	□ Cold Start	
	□ LinkUp	□ LinkDown	
WAE Alarm:	□ Raise Critical	□ Clear Critical	
	□ Raise Major	□ Clear Major	
	□ Raise Minor	□ Clear Minor	
Entity:	□		
Event:	□		
Config:	□		

Miscellaneous Settings

MIB Persistent Event:	□
Notify Inform:	□

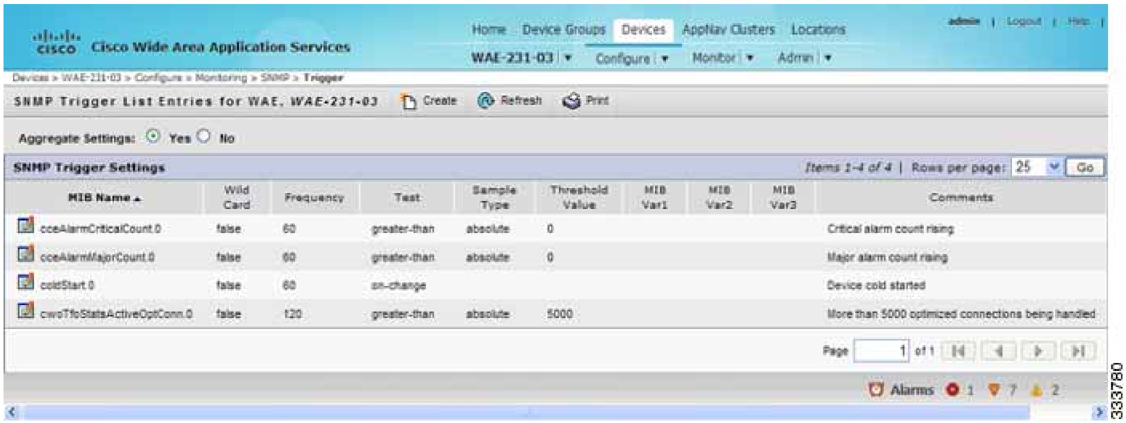
Viewing SNMP Trigger Lists

To view the list of SNMP trap triggers defined for a device or group, 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** > **SNMP** > **Trigger**. The SNMP Trigger List window appears. See Figure 3-2.

Figure 3-2 *SNMP Trigger List Window*



SNMP Trigger List Entries for WAE, WAE-231-03

Aggregate Settings: ● Yes ○ No

SNMP Trigger Settings

MIB Name ▲	Wild Card	Frequency	Test	Sample Type	Threshold Value	MIB Var1	MIB Var2	MIB Var3	Comments
cceAlarmCriticalCount.0	false	60	greater-than	absolute	0				Critical alarm count rising
cceAlarmMajorCount.0	false	60	greater-than	absolute	0				Major alarm count rising
coldStart.0	false	60	on-change						Device cold started
cwoTfoStatsActiveOptConn.0	false	120	greater-than	absolute	5000				More than 5000 optimized connections being handled

For more information about SNMP Triggers, see the "Configuring SNMP Monitoring" chapter in the *Cisco Wide Area Application Services Configuration Guide*.

Defining New Traps

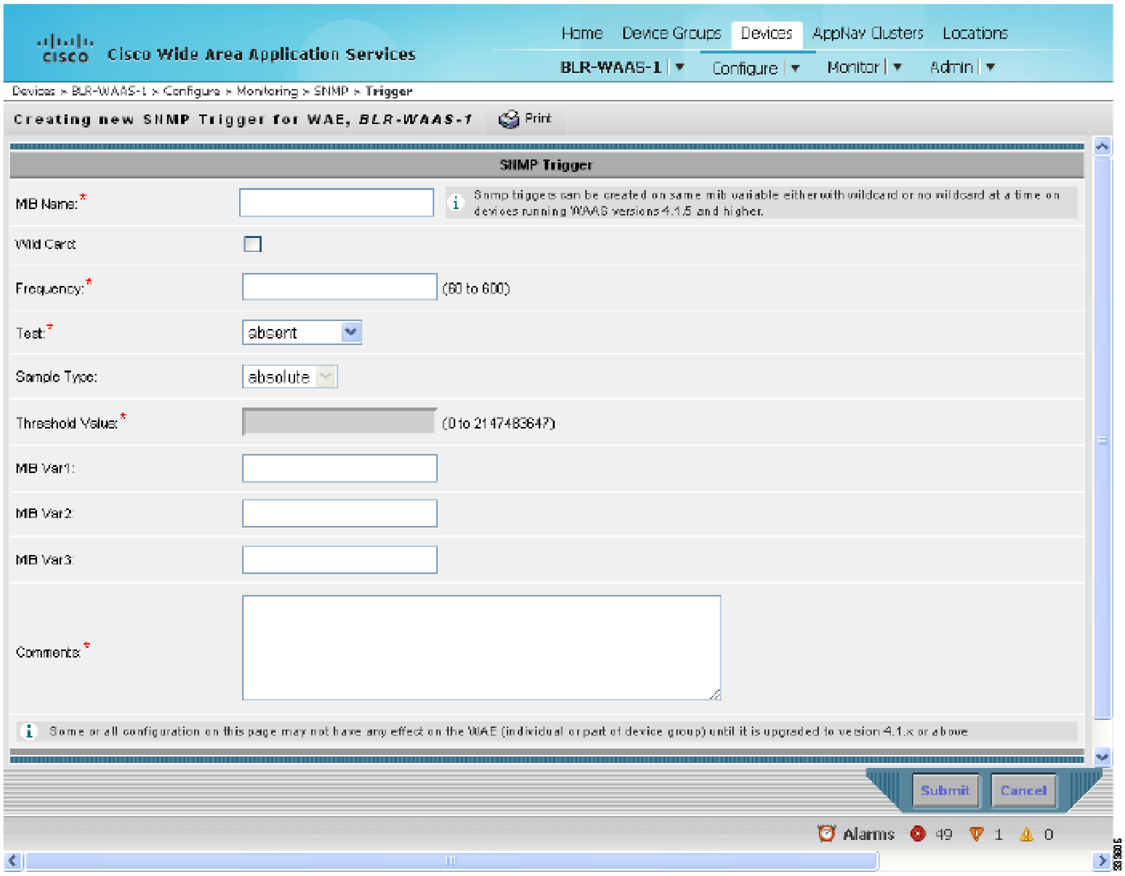
To add a new SNMP trap on a WAAS device or device group, follow these steps:

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

Step 2 Choose **Configure** > **Monitoring** > **SNMP** > **Trigger**. The SNMP Trigger List window appears. See Figure 3-2.

Step 3 In the Trigger list window, click **Create**. The SNMP Trigger window appears. See Figure 3-3.

Figure 3-3 SNMP Trigger Window



Devices > BLR-WAAS-1 > Configure > Monitoring > SNMP > Trigger

Creating new SNMP Trigger for WAE, *BLR-WAAS-1*

SNMP Trigger

MIB Name:*	Snmp triggers can be created on same mib variable either with wildcard or no wildcard at a time on devices running WAAS versions 4.1.5 and higher.
Wild Card:	□
Frequency:*	(60 to 600)
Test:*	absent
Sample Type:	absolute
Threshold Value:*	(0 to 2147483647)
MIB Var1:	
MIB Var2:	
MIB Var3:	
Comments:*	

Some or all configuration on this page may not have any effect on the WAE (individual or part of device group) until it is upgraded to version 4.1.x or above

Step 4 Define the trigger settings.

Step 5 Click **Submit**.

Information About Common SNMP MIB OIDS

This section describes some of the common SNMP trap Object Identifiers (OIDs) that you might see:

- cceAlarmCriticalRaised OID, page 3-6
- coldStart OID, page 3-7
- cceAlarmCriticalCleared OID, page 3-7
- cceFailedDiskName OID, page 3-8
- ciscoContentEngineDiskFailed OID, page 3-8

cceAlarmCriticalRaised OID

The cceAlarmCriticalRaisedOID trap signifies that a module raised a Critical alarm.

Object	**cceAlarmCriticalRaised**
OID	**1.3.6.1.4.1.9.9.178.2.0.7**
Status	**current**
MIB	**CISCO-CONTENT-ENGINE-MIB**; View Supporting Images
Trap Components	**cceAlarmHistId** **cceAlarmHistModuleId** **cceAlarmHistCategory** **cceAlarmHistInfo** **cceAlarmHistTimeStamp**

coldStart OID

The coldStart trap signifies that the SNMP entity, supporting a notification originator application, is reinitializing itself and that its configuration may have been altered.

Object	**coldStart**
OID	**1.3.6.1.6.3.1.1.5.1**
Status	**current**
MIB	**SNMPv2-MIB**; View Supporting Images

cceAlarmCriticalCleared OID

The cceAlarmCriticalRaisedOID trap signifies that a module cleared a Critical alarm.

Object	**cceAlarmCriticalCleared**
OID	**1.3.6.1.4.1.9.9.178.2.0.8**
Status	**current**

MIB	**CISCO-CONTENT-ENGINE-MIB**; View Supporting Images
Trap Components	**cceAlarmHistId** **cceAlarmHistModuleId** **cceAlarmHistCategory** **cceAlarmHistInfo** **cceAlarmHistTimeStamp**

cceFailedDiskName OID

The cceFailedDiskNameOID trap signifies that a disk failure event occurred and includes the name of that disk.

Object	**cceFailedDiskName**
OID	**1.3.6.1.4.1.9.9.178.1.5.1**
Type	**OCTET STRING**
Permission	**accessible-for-notify**
Status	**current**
MIB	**CISCO-CONTENT-ENGINE-MIB**; View Supporting Images

ciscoContentEngineDiskFailed OID

The ciscoContentEngineDiskFailed trap signifies that a Content Engine data drive failed. This object supersedes ciscoContentEngineDataDiskFailed. Additional information about the error is logged to syslog.

Object	**ciscoContentEngineDiskFailed**
OID	**1.3.6.1.4.1.9.9.178.2.0.6**
Status	**current**
MIB	**CISCO-CONTENT-ENGINE-MIB**; View Supporting Images
Trap Components	**cceFailedDiskName**

CHAPTER 4

Monitoring WAAS Using XML API

This chapter describes how to use the WAAS API to monitor your WAAS devices and how to use soapUI with the WAAS API interface.

This chapter contains the following sections:

Information About the XML-Based API

The WAAS Central Manager Web Service provides an XML-based API that supports monitoring device status and information, alarms, and statistics. It does not support device configuration.

For more information about the XML API, see the *Cisco Wide Area Application Services API Reference*.

The following services are offered:

- AppNav Statistics Service (AppNavStats)
- CIFS Statistics Service (CIFSStats)
- Device Configuration Service (DeviceConf)
- Events Service (AlarmStatus)
- HTTP and HTTPS Statistics Service (HttpStats and HttpsStats)
- ICA Statistics Service (ICAStats)
- MAPI Statistics Service (MapiStats)
- NFS Statistics Service (NfsStats)
- SMB Statistics Service (SmbStats)
- SSL Statistics Service (SSLStats)
- Status Service (DeviceStatus)
- Traffic Acceleration Service (TrafficStats)
- Video Streaming Statistics Service (VideoStats)

To obtain the WSDL file defined for a particular service in the WAAS Central Manager monitoring API implementation, you submit a URL to the service with a ?wsdl suffix as follows:

https://<host/ip>:8443/ws/s*ervice_name*?wsdl

To query a service for information, you send an XML-formatted SOAP request to the service at the following URL:

https://<host/ip>:8443/ws/*service_name*

Using the Traffic Acceleration Service

You can retrieve traffic and application statistics for individual WAEs, device groups, and for the WAAS network using the Traffic Acceleration service (TrafficStats Web Service), which performs actions that include the following:

- getAllClassMap—Retrieves all of the monitored class map names.
- getMonitoredApplications—Retrieves a list of all types of applications known in the scope of the system.
- retrieveAppTrafficStats—Retrieves overall traffic statistics collected on either a WAAS device, WAEs within a device group, or all system-wide WAEs. The traffic is further filtered based on the specified application names
- retrieveAverageThroughPutClassStats—Retrieves average throughput counts for a set of class map names.
- retrieveAverageThroughPutStats—Retrieves the average throughput values collected on a device.
- retrieveClassTrafficStats—Retrieves traffic byte counts for the specified class map names.
- retrieveConnection—Retrieves overall connection details for the current time.
- retrieveConnectionTrendClassStats—Retrieves overall connection trend details of applications collected on a device.
- retrieveConnectionTrendStats—Retrieves connection counts for the specified set of class map names.
- retrieveCPUUtilization—Retrieves the CPU utilization information for a specified WAE.
- retrievePeakThroughPutClassStats—Retrieves peak throughput values for the specified set of class map names.
- retrievePeakThroughPutStats—Retrieves the peak throughput values collected on a device.
- retrieveTrafficStats—Retrieves the overall statistics collected on either a WAAS device, WAEs within a device group, or all system-wide WAEs.

Using the Events and Status Service

You can retrieve alarm information, device status, and disk status using the Events and Status service (AlarmStatus Web Service), which performs one or more of the following actions:

- getDeviceStatus—Retrieves the device status.
- getDiskEncryptStatus—Retrieves the disk encryption status.
- getDiskInformation—Retrieves information about the disk.

- getDiskStatus—Retrieves the physical disk status.
- getMonitoredAOsByWaeIDs—Retrieves the operational status of application accelerators for a list of device IDs.
- getMonitoredAOs—Retrieves the operational status of application accelerators for either a WAAS device, WAEs within a device group, or all system-wide WAEs.
- retrieveAlarmByName—Retrieves a list of all alarms filtered by the name of the WAE or WAE group, the object type, or the alarm name.
- retrieveAlarmBySeverity—Retrieves a list of all active alarms for the specified WAE or WAE group, further filtered on alarm severity.
- retrieveAllAlarms—Retrieves all alarms.

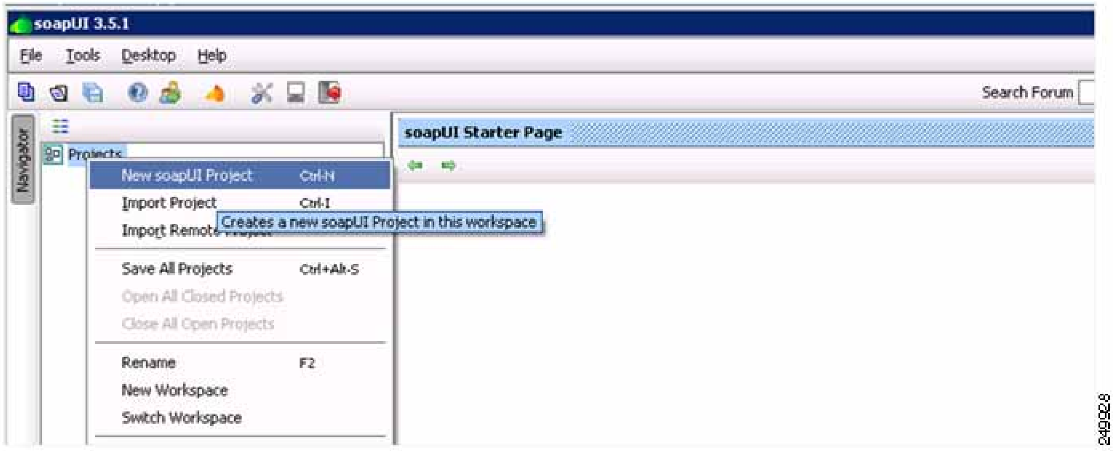
Using soapUI to Access the WAAS API Interface

You can access the WAAS API interface using third-party tools such as soapUI, WebInject, ApacheCXF, and so forth. The soapUI website (http://www.soapui.org/) offers a free software version that you can download and install on a client PC. The procedure in this section describes how to create a project using soapUI after you install and start the software.

Procedure

Step 1 Right-click **Projects** and click **New soapUI Project** to create a project (for example, WAAS-Project). See Figure 4-1.

Figure 4-1 soapUI: Create New Project



The New soapUI Project dialog box appears.

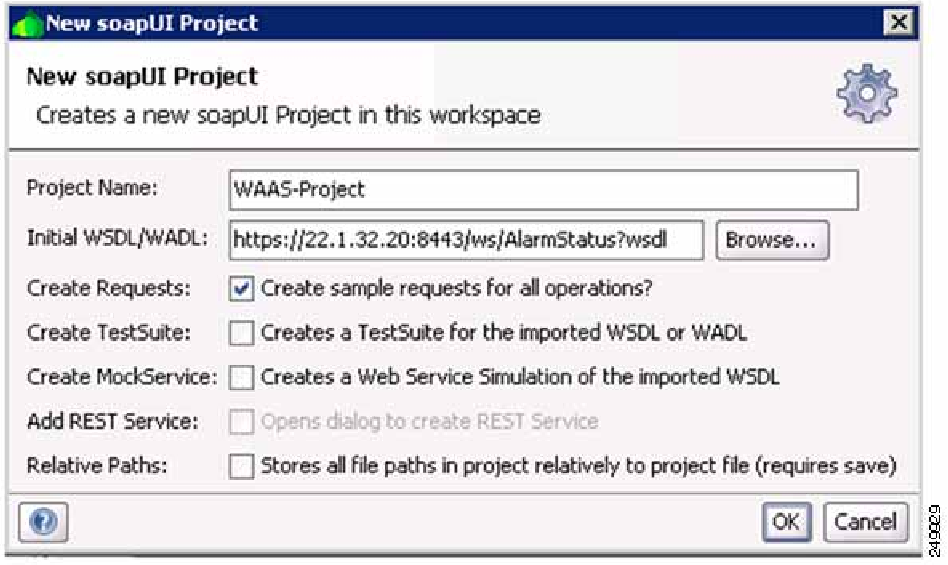
Step 2 From the New soapUI Project dialog box (see Figure 4-2), do the following:

a. Enter the WSDL URL.

b. Check the **Create Requests** check box.

c. Click **Ok**. A progress window appears while the data is gathered, which may take several seconds to load.

Figure 4-2 soapUI: New Project Dialog Box



New soapUI Project

New soapUI Project
Creates a new soapUI Project in this workspace

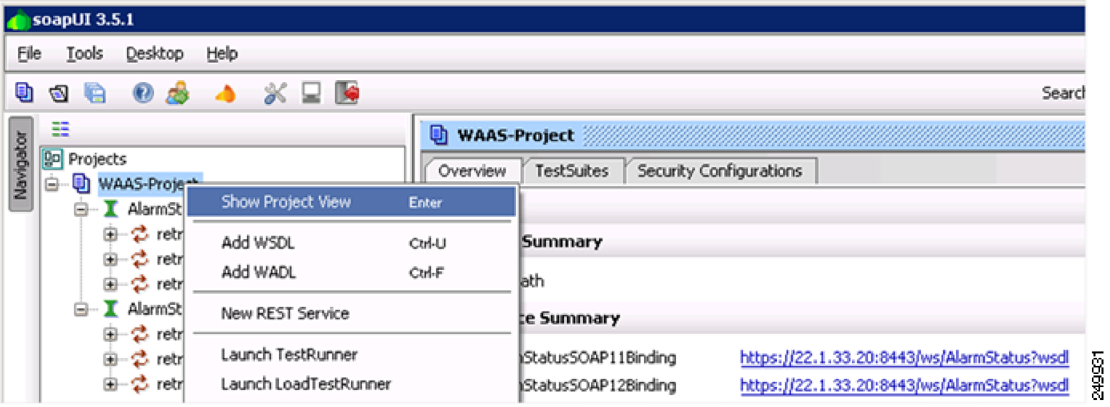
Project Name: WAAS-Project
Initial WSDL/WADL: https://22.1.32.20:8443/ws/AlarmStatus?wsdl
Create Requests: ☑ Create sample requests for all operations?
Create TestSuite: □ Creates a TestSuite for the imported WSDL or WADL
Create MockService: □ Creates a Web Service Simulation of the imported WSDL
Add REST Service: □ Opens dialog to create REST Service
Relative Paths: □ Stores all file paths in project relatively to project file (requires save)

After the WSDL loads, the available navigation options appear.

Step 3 Specify security credentials by doing the following:

a. Right-click the new project (such as WAAS-Project) and click **Show Project View**. See Figure 4-3.

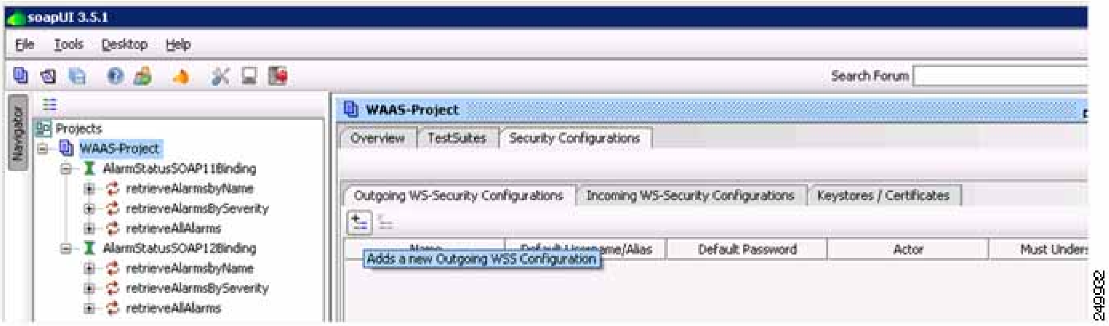
Figure 4-3 soapUI: Show Project View



The WAAS-Project pane appears.

b. From the WAAS-Project pane, add a new WSS by clicking the **Security Configurations** tab and click the plus sign (+) below the Outgoing WS-Security Configurations tab. See Figure 4-4)

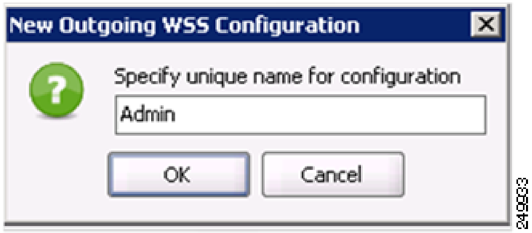
Figure 4-4 soapUI: Add New WSS



The New Outgoing WSS Configuration dialog box appears.

c. From the New Outgoing WSS Configuration dialog box, enter a name for the new WSS (such as Admin) and click **OK**. See Figure 4-5.

Figure 4-5 soapUI: New Outgoing WSS Configuration Dialog Box

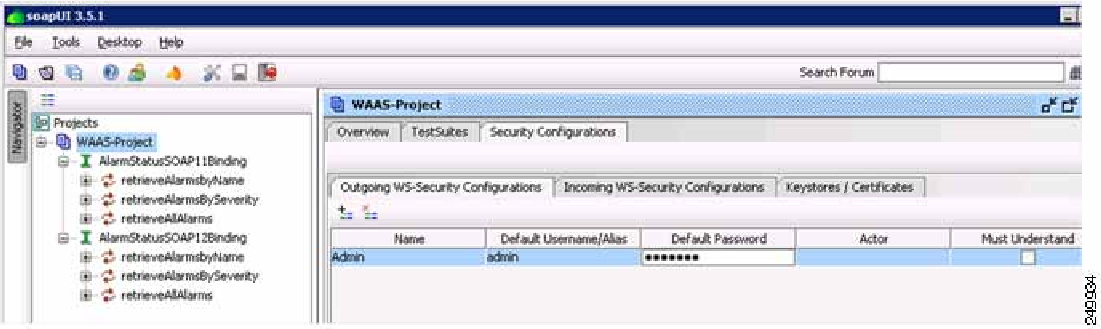

New Outgoing WSS Configuration
Specify unique name for configuration
OK
Cancel
249933

Admin

The dialog box closes and the Outgoing WS-Security Configuration tab displays the new WSS.

d. From the Outgoing WS-Security Configuration tab, enter the device username and password. See Figure 4-6.

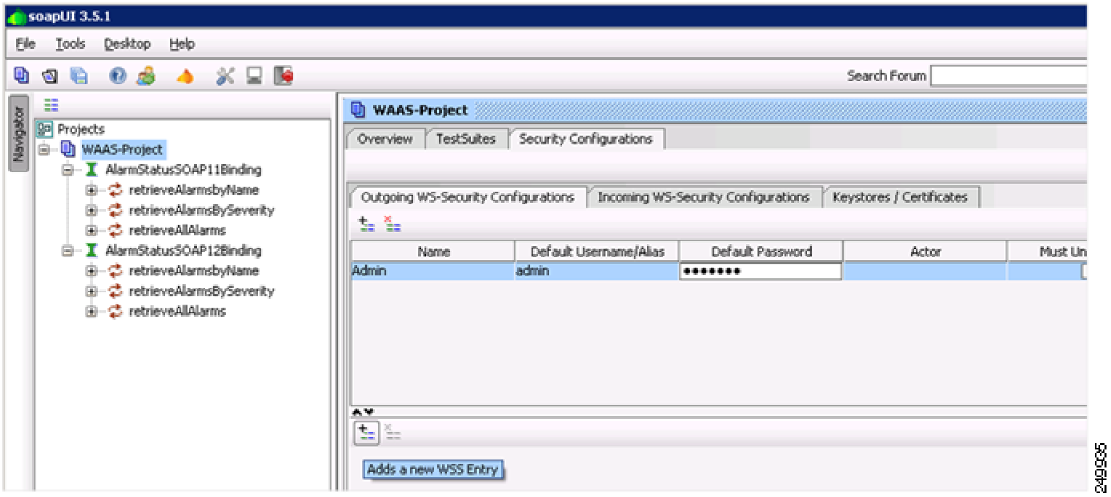
Figure 4-6 soapUI: WSS Username and Password



Name	Default Username/Alias	Default Password	Actor	Must Understand
Admin	admin	•••••••		□

e. Click the plus sign (+) in the lower pane to add a new WSS Entry. See Figure 4-7.

Figure 4-7 soapUI: Add WSS Entry

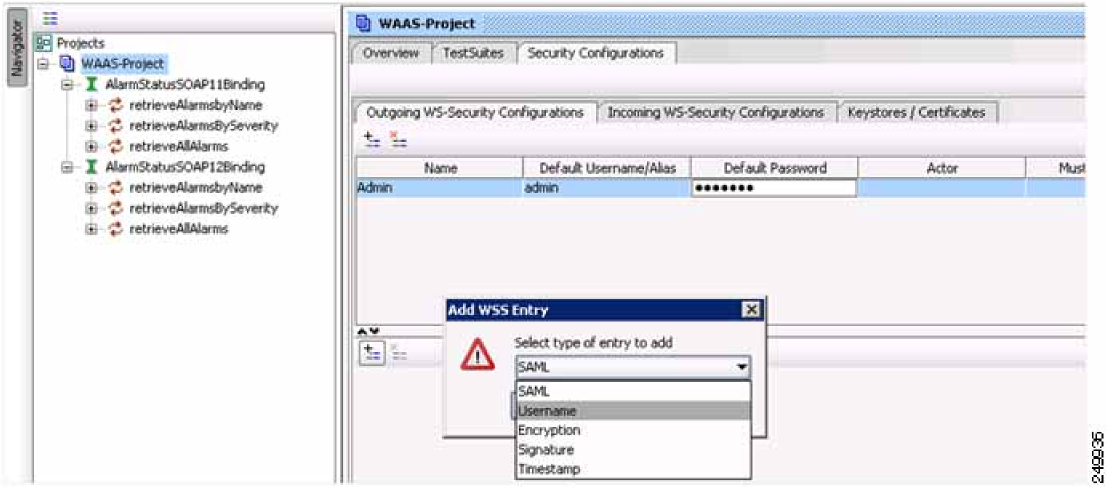


Name	Default Username/Alias	Default Password	Actor	Must Un
Admin	admin	•••••••		

The Add WSS Entry dialog box appears.

f. From the Select Type of Entry to Add drop-down list, choose **Username**. See Figure 4-8.

Figure 4-8 soapUI: Add WSS Entry



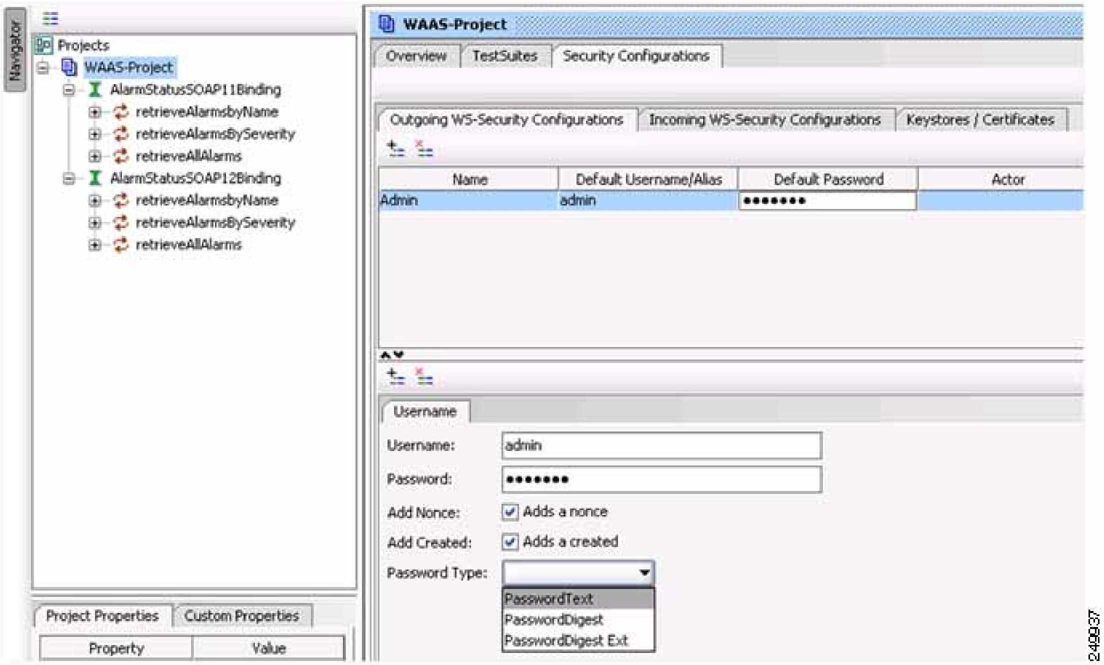
Name	Default Username/Alias	Default Password	Actor	Must
Admin	admin	•••••••		

Select type of entry to add: SAML

The dialog box closes and the lower pane of the Outgoing WS-Security Configuration tab displays the Username tab with your username and password already populated.

g. From the Username tab’s Password Type drop-down list, choose **PasswordText**. See Figure 4-9.

Figure 4-9 soapUI: Password Type



Name	Default Username/Alias	Default Password	Actor
Admin	admin	•••••••	

Username: admin

Password: •••••••

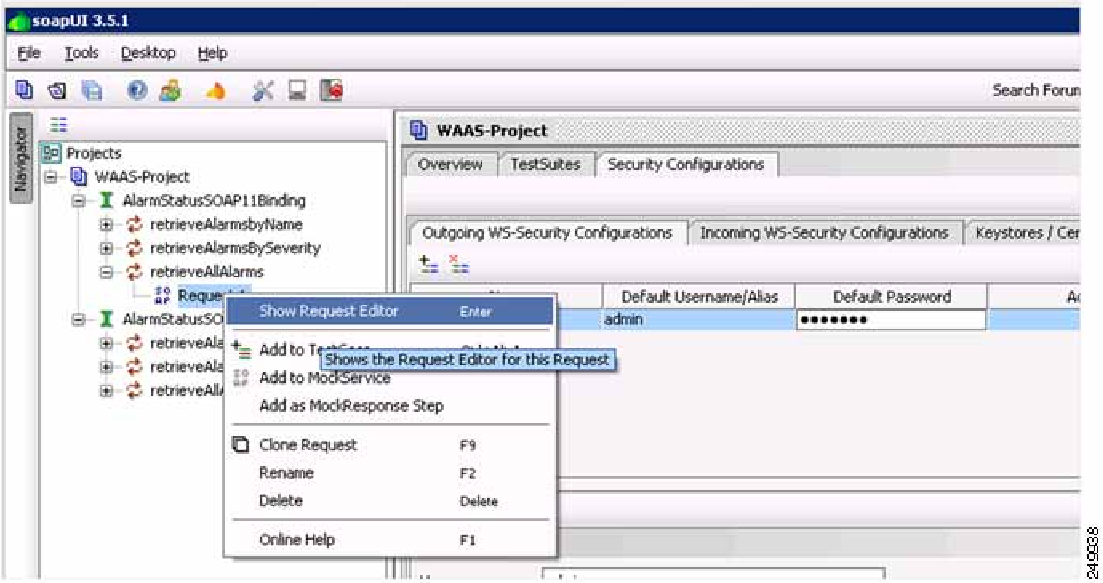
Add Nonce: ☑ Adds a nonce

Add Created: ☑ Adds a created

Password Type:

Step 4 From the Projects tree on the left, click **+** to expand one of the listed items, double-click **Request x** to display the drop-down list, and choose **Show Request Editor** from the menu. See Figure 4-10.

Figure 4-10 soapUI: Show Request Editor

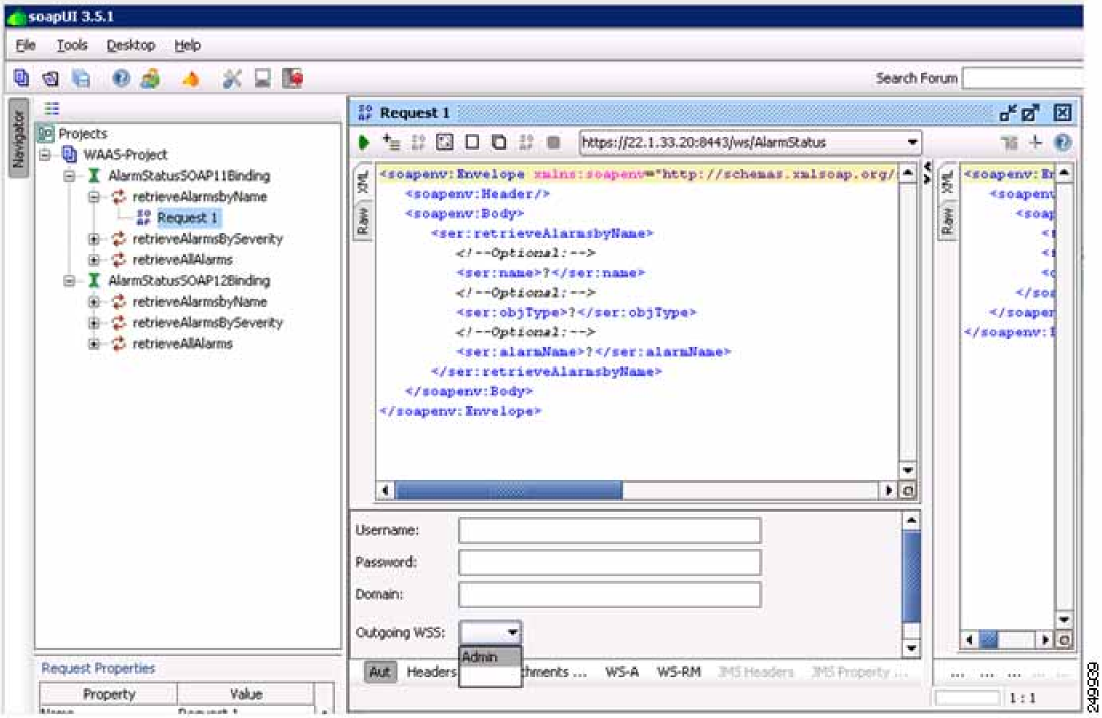


Default Username/Alias	Default Password
admin	•••••••

The Request Editor pane appears.

Step 5 From the Request Editor pane, click **Aut** at the bottom and choose **Admin** from the Outgoing WSS drop-down list. See Figure 4-11.

Figure 4-11 soapUI: Request Editor



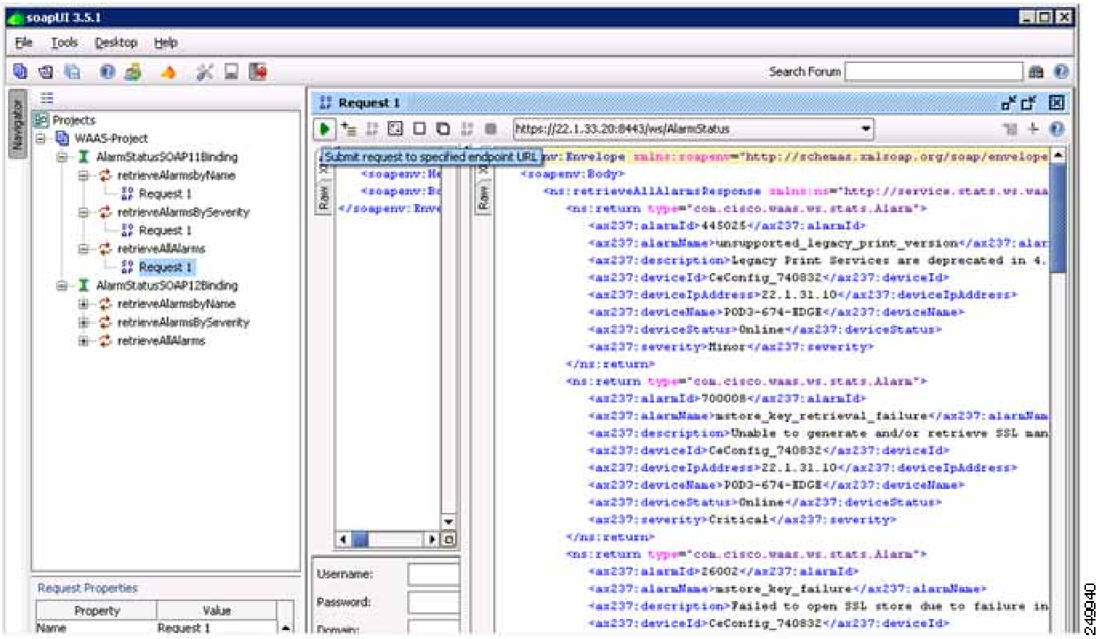
https://22.1.33.20:8443/ws/AlarmStatus

```
<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/
   <soapenv:Header/>
   <soapenv:Body>
      <ser:retrieveAlarmsbyName>
         <!--Optional:-->
         <ser:name>?</ser:name>
         <!--Optional:-->
         <ser:objType>?</ser:objType>
         <!--Optional:-->
         <ser:alarmName>?</ser:alarmName>
      </ser:retrieveAlarmsbyName>
   </soapenv:Body>
</soapenv:Envelope>
```

Step 6 Verify the WSDL URL and click **Submit** to query the device.

After the request is complete, the data in XML format appears. See Figure 4-12.

Figure 4-12 soapUI: Data in XML Format



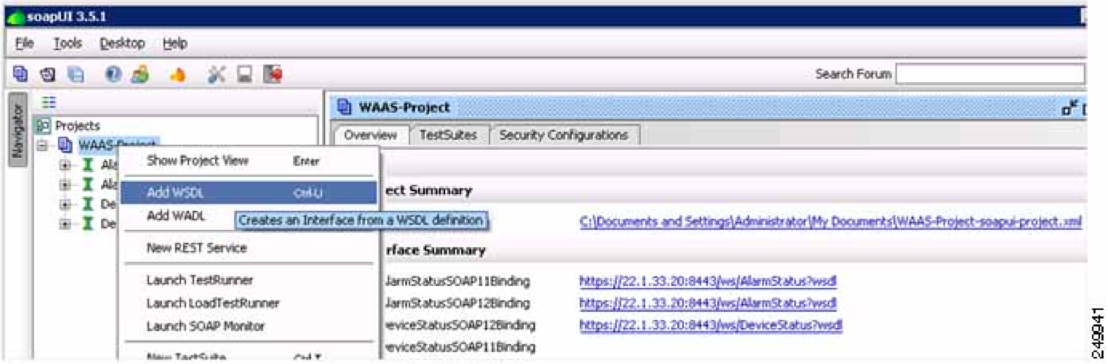
https://22.1.33.20:8443/ws/AlarmStatus

```
<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope
   <soapenv:Body>
      <ns:retrieveAllAlarmsResponse xmlns:ns="http://service.stats.ws.waa
         <ns:return type="com.cisco.waas.ws.stats.Alarm">
            <ax237:alarmId>445025</ax237:alarmId>
            <ax237:alarmName>unsupported_legacy_print_version</ax237:alar
            <ax237:description>Legacy Print Services are deprecated in 4.
            <ax237:deviceId>CeConfig_740832</ax237:deviceId>
            <ax237:deviceIpAddress>22.1.31.10</ax237:deviceIpAddress>
            <ax237:deviceName>POD3-674-EDGE</ax237:deviceName>
            <ax237:deviceStatus>Online</ax237:deviceStatus>
            <ax237:severity>Minor</ax237:severity>
         </ns:return>
         <ns:return type="com.cisco.waas.ws.stats.Alarm">
            <ax237:alarmId>700008</ax237:alarmId>
            <ax237:alarmName>mstore_key_retrieval_failure</ax237:alarmNam
            <ax237:description>Unable to generate and/or retrieve SSL man
            <ax237:deviceId>CeConfig_740832</ax237:deviceId>
            <ax237:deviceIpAddress>22.1.31.10</ax237:deviceIpAddress>
            <ax237:deviceName>POD3-674-EDGE</ax237:deviceName>
            <ax237:deviceStatus>Online</ax237:deviceStatus>
            <ax237:severity>Critical</ax237:severity>
         </ns:return>
         <ns:return type="com.cisco.waas.ws.stats.Alarm">
            <ax237:alarmId>26002</ax237:alarmId>
            <ax237:alarmName>mstore_key_failure</ax237:alarmName>
            <ax237:description>Failed to open SSL store due to failure in
            <ax237:deviceId>CeConfig_740832</ax237:deviceId>
```

```
<soapenv:He
<soapenv:Bo
</soapenv:Enve
```

Step 7 (Optional) To add more WSDL, right-click the project to display the drop-down list and choose **Add WSDL** from the menu. See Figure 4-13.

Figure 4-13 soapUI: Add WSDL



CHAPTER 5

Monitoring WAAS Using Cisco Network Analysis Module

This chapter describes Cisco Network Analysis Module (NAM), which you can use to monitor your WAAS devices.

This chapter contains the following sections:

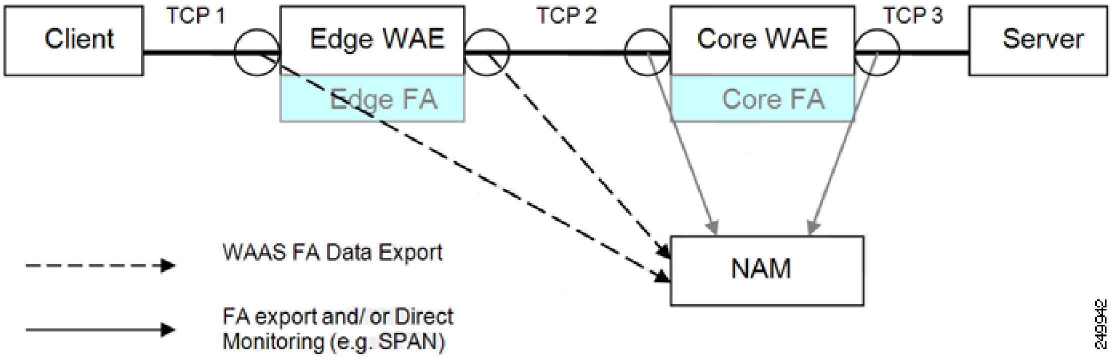
- Information About NAM, page 5-1
- Configuring NAM Monitoring of WAAS Devices, page 5-3
- NAM Deployment Scenarios, page 5-6
- Monitoring and Analyzing Traffic Using the NAM, page 5-7

Information About NAM

NAM monitors network and application response time (ART) by analyzing the exchanges of TCP packets between clients and application servers. The NAM Traffic Analyzer software enables network managers to understand, manage, and improve how applications and services are delivered to end users by combining flow-based and packet-based analysis into one solution.

The Cisco NAM includes an embedded, web-based Traffic Analyzer GUI that provides quick access to the configuration menus and presents easy-to-read performance monitoring and analysis on network traffic. A FlowAgent (FA) runs on WAAS devices to collect TCP packet data and send the flow data to NAM for analyzing and reporting. See Figure 5-1.

Figure 5-1 NAM Monitoring of WAAS Devices



For more information about NAM, see the following documentation URLs:

- Complete NAM documentation set:

  http://www.cisco.com/en/US/products/sw/cscowork/ps5401/tsd_products_support_series_home.html
- *Cisco WAAS NAM Virtual Service Blade Installation and Configuration Guide*:

  http://www.cisco.com/en/US/products/sw/cscowork/ps5401/prod_installation_guides_list.html

Information About NAM Monitoring Functions

NAM provides the following monitoring functions:

- Monitoring Client-Edge Connections—By monitoring the TCP connections between the clients and the WAAS edge device (connection TCP-1 in Figure 5-1), the following ART metrics can be measured:
  - Total Delay (TD) as experienced by the client
  - Total Transaction Time as experienced by the client
  - Bandwidth usage (bytes/packets) before compression
  - Number of transactions and connections
  - Network round-trip time (RTT) broken down into two segment: client-edge and edge-server
- Monitoring Edge-Core Optimized Connections—By monitoring the spoofed TCP connections between the edge and core WAAS devices (connection TCP-2 in Figure 5-1), the following additional ART metric can be measured: Bandwidth usage (bytes/packets) after compression.
- Monitoring Edge-Core Connections—By monitoring the TCP connections between the core WAAS devices and the servers (connection TCP-3 in Figure 5-1), additional ART metrics can be measured:
  - Application (Server) Delay (without the proxy acceleration/caching server)
  - Network RTT between the core WAAS device and the servers

The sections that follow show how to configure WAAS to enable monitoring by NAM and how to configure NAM to monitor specific WAAS functions.

Configuring NAM Monitoring of WAAS Devices

This section contains the following topics:

- Configuring Basic WAAS Setup, page 5-3
- Configuring WAAS Monitored Servers, page 5-4
- Configuring WAAS Data Sources in NAM, page 5-5

Configuring Basic WAAS Setup

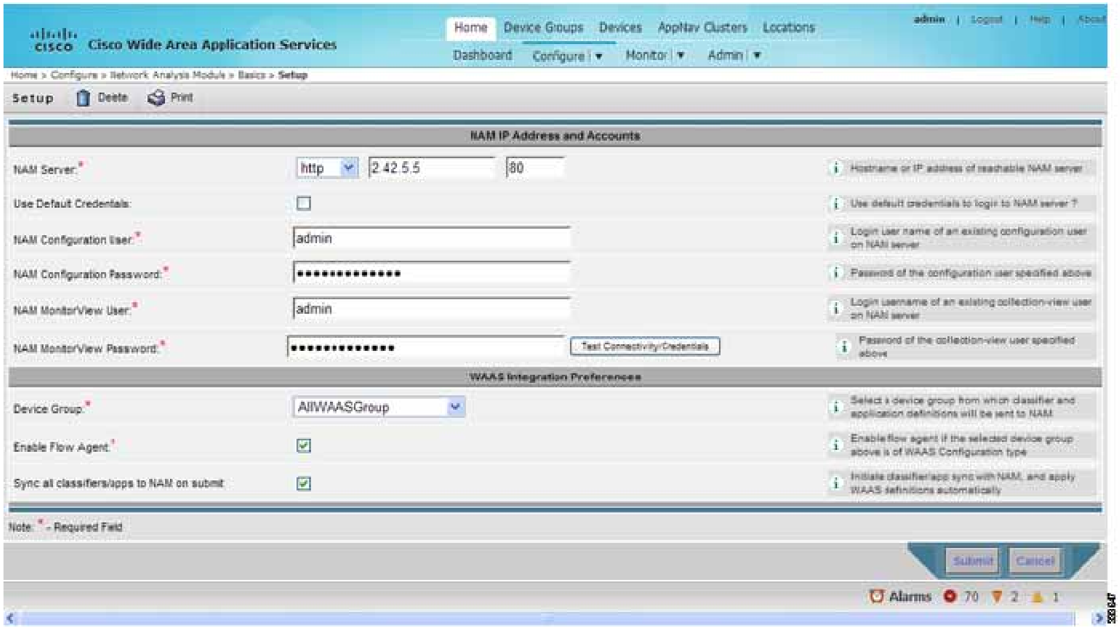
Before you can monitor WAAS traffic, you must first set up basic NAM configuration by completing the following tasks:

- Connect to a NAM server by providing the server's IP address, protocol, and port.
- Establish account credentials.
- Associate a WAAS device group or WAAS Express device group with configured policies.
- Enable Flow Agent.

Follow the steps below to complete basic NAM configuration. Only device group level policy configurations are applicable for NAM.

Step 1 From the WAAS Central Manager, choose **Configure** > **Network Analysis Module** > **Basics** > **Setup.** The Setup window appears. (See Figure 5-2).

Figure 5-2 NAM Setup Window


Cisco Wide Area Application Services
Home
Device Groups
Devices
AppNav Clusters
Locations
Dashboard
Configure
Monitor
Admin
admin | Logout | Help | About
Home > Configure > Network Analysis Module > Basics > Setup
Setup
Delete
Print
Submit
Cancel
Alarms 70 2 1

NAM IP Address and Accounts

NAM Server:*	http 2.42.5.5 80	Hostname or IP address of reachable NAM server
Use Default Credentials:	□	Use default credentials to login to NAM server ?
NAM Configuration User:*	admin	Login user name of an existing configuration user on NAM server
NAM Configuration Password:*	••••••••••••••	Password of the configuration user specified above
NAM MonitorView User:*	admin	Login username of an existing collection-view user on NAM server
NAM MonitorView Password:*	•••••••••••••• Test Connectivity/Credentials	Password of the collection-view user specified above

WAAS Integration Preferences

Device Group:*	AllWAASGroup	Select a device group from which classifier and application definitions will be sent to NAM
Enable Flow Agent:*	☑	Enable flow agent if the selected device group above is of WAAS Configuration type
Sync all classifiers/apps to NAM on submit:	☑	Initiate classifier/app sync with NAM, and apply WAAS definitions automatically

Note: * - Required Field

Step 2 Choose either **HTTP** or **HTTPS**, depending on which access was configured during NAM installation.

Step 3 Enter the hostname and IP address of the NAM server.

Step 4 Configure the credentials: use the preconfigured login credentials by selecting the **Use Default Credentials** option, or configure the credentials manually by filling in the fields with valid values.

Step 5 Configure the WAAS Integration Preferences to configure a WAAS device group to work with the NAM server as follows:

a. Choose the device group from which applications and classifier definitions are pushed to the NAM when performing a synchronization operation.

b. Choose the **Enable Flow Agent** option to data export.

c. Choose the **Sync all classifiers/apps to NAM on submit** to initiate synchronization with the NAM.

Step 6 Click **Submit**.

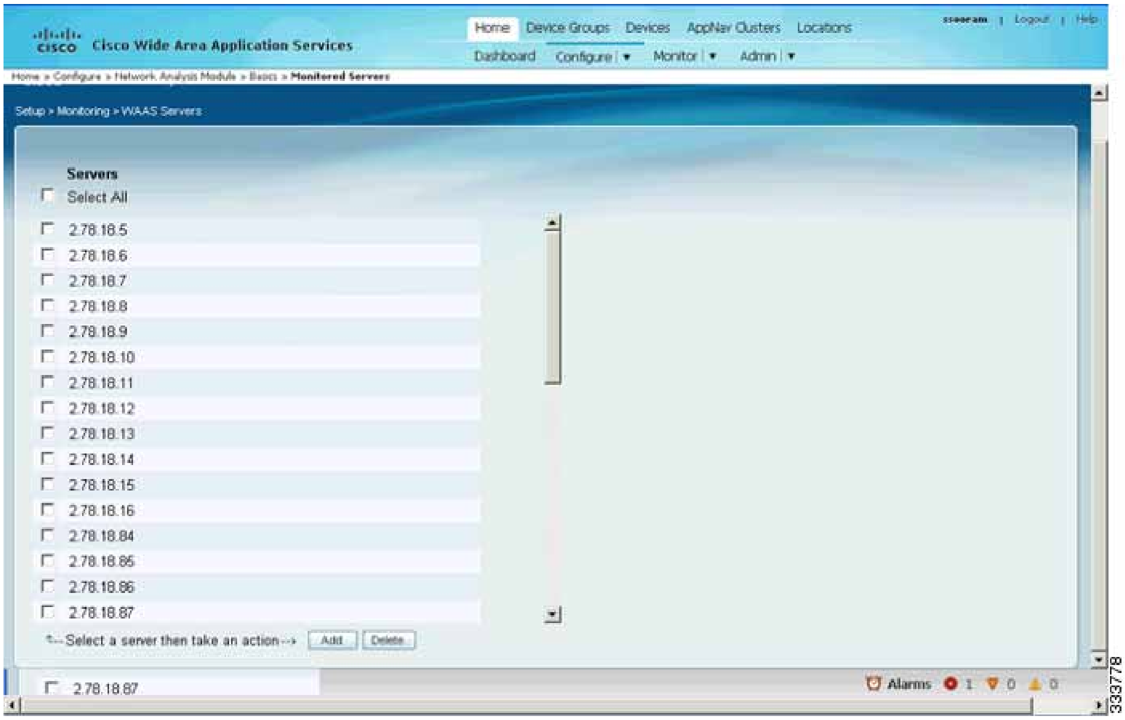
For additional information about configuring NAM, see the NAM chapter in the *Cisco Wide Area Application Services Configuration Guide*.

Configuring WAAS Monitored Servers

To monitor the response time for a server, you need to add the server IP address in the NAM configuration setup, as follows:

Step 1 From the WAAS Central Manager menu, choose **Configure** > **Network Analysis Module** > **Basics** > **Monitored Servers**. The NAM WAAS Servers Monitoring window appears. See Figure 5-3.

Figure 5-3 WAAS Servers Monitoring Window


Cisco Wide Area Application Services
Home
Device Groups
Devices
AppNav Clusters
Locations
Dashboard
Configure ▾
Monitor ▾
Admin ▾
Logout
Help
Home » Configure » Network Analysis Module » Basics » Monitored Servers
Setup » Monitoring » WAAS Servers
Add
Delete
Alarms ● 1 ▼ 0 ▲ 0
333778

Servers

□ Select All

□ 2.78.18.5
□ 2.78.18.6
□ 2.78.18.7
□ 2.78.18.8
□ 2.78.18.9
□ 2.78.18.10
□ 2.78.18.11
□ 2.78.18.12
□ 2.78.18.13
□ 2.78.18.14
□ 2.78.18.15
□ 2.78.18.16
□ 2.78.18.84
□ 2.78.18.85
□ 2.78.18.86
□ 2.78.18.87

←Select a server then take an action→

□ 2.78.18.87

Step 2 Choose the IP address of one or more servers to monitor.

Step 3 Click **Add**. The Add WAAS Servers(s) window appears.

Step 4 Click **Submit** to add the server IP address(es).

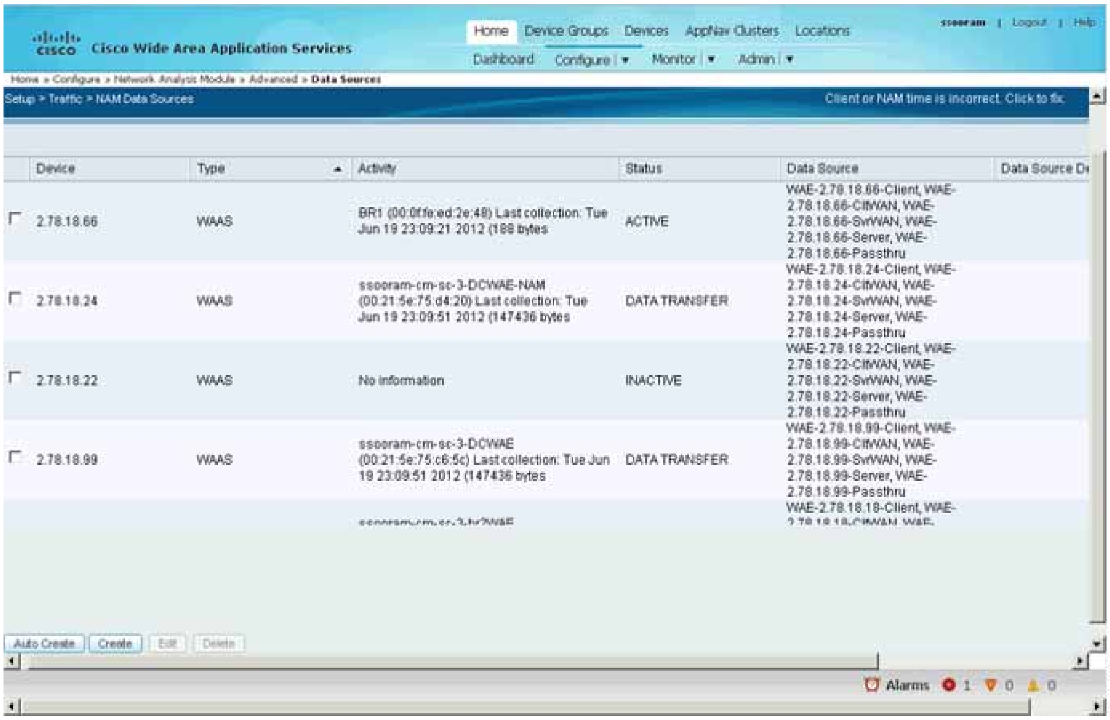
Configuring WAAS Data Sources in NAM

You usually don't need to add WAAS devices because export-enabled WAAS devices are detected and added automatically.

To manually add a WAAS device to the list of devices monitored by NAM, follow these steps:

Step 1 From the WAAS Central Manager menu, choose **Configure** > **Network Analysis Module** > **Basics** > **Monitored Servers**. The NAM Data Source Configuration window appears. (See Figure 5-4).

Figure 5-4 NAM Data Sources


Cisco Wide Area Application Services
Home
Device Groups
Devices
AppNav Clusters
Locations
ssooram
Logout
Help
Dashboard
Configure
Monitor
Admin
Home » Configure » Network Analysis Module » Advanced » Data Sources
Setup > Traffic > NAM Data Sources
Client or NAM time is incorrect. Click to fix
Auto Create
Create
Edit
Delete
Alarms
1
0
0
333777

	Device	Type	Activity	Status	Data Source	Data Source D
□	2.78.18.66	WAAS	BR1 (00:0f:fe:ed:2e:48) Last collection: Tue Jun 19 23:09:21 2012 (188 bytes	ACTIVE	WAE-2.78.18.66-Client, WAE-2.78.18.66-CifWAN, WAE-2.78.18.66-SvrWAN, WAE-2.78.18.66-Server, WAE-2.78.18.66-Passthru	
□	2.78.18.24	WAAS	ssooram-cm-sc-3-DCWAE-NAM (00:21:5e:75:d4:20) Last collection: Tue Jun 19 23:09:51 2012 (147436 bytes	DATA TRANSFER	WAE-2.78.18.24-Client, WAE-2.78.18.24-CifWAN, WAE-2.78.18.24-SvrWAN, WAE-2.78.18.24-Server, WAE-2.78.18.24-Passthru	
□	2.78.18.22	WAAS	No information	INACTIVE	WAE-2.78.18.22-Client, WAE-2.78.18.22-CifWAN, WAE-2.78.18.22-SvrWAN, WAE-2.78.18.22-Server, WAE-2.78.18.22-Passthru	
□	2.78.18.99	WAAS	ssooram-cm-sc-3-DCWAE (00:21:5e:75:c6:5c) Last collection: Tue Jun 19 23:09:51 2012 (147436 bytes	DATA TRANSFER	WAE-2.78.18.99-Client, WAE-2.78.18.99-CifWAN, WAE-2.78.18.99-SvrWAN, WAE-2.78.18.99-Server, WAE-2.78.18.99-Passthru	
			ssooram-cm-sc-3-br2WAE		WAE-2.78.18.18-Client, WAE-2.78.18.18-CifWAN, WAE-	

Step 2 From the list of Types, choose **WAAS** device.

Step 3 In the IP field, enter the device IP address.

Step 4 Check the check boxes for the data sources that you want to monitor. See Table 5-1 for more information.

Step 5 Click **Submit** to add the new data source.

Table 5-1 WAAS Data Sources

WAAS Data Source	Description
Client	Export the original (LAN side) TCP flows originated from its clients to NAM for monitoring.
Client WAN	Export the optimized (WAN side) TCP flows originated from its clients to NAM for monitoring.
Server WAN	Export the optimized (WAN side) TCP flows from its servers to NAM for monitoring.
Server	Export the original (LAN side) TCP flows from its servers to NAM for monitoring.
Pass-Through	Export the flows that traverses WAAS without being optimized.

For additional information about configuring and using NAM, see the *User Guide for Cisco Network Analysis Module Traffic Analyzer.*

NAM Deployment Scenarios

The NAM uses WAAS data sources to monitor traffic collected from different WAAS segments: Client, Client WAN, Server WAN, and Server. Each WAAS segment is represented by a data source. You can set up the NAM to monitor and report other traffic statistics of the WAAS data sources (such as application, host, and conversation information) in addition to the monitored ART metrics.

The use of the data source depends upon on the WAAS deployment scenario. Table 5-2 describes several common WAAS deployment scenarios and their applicable data sources.

Table 5-2 WAAS Deployment Scenarios

Deployment Scenario	Edge WAE Data Source	Core WAE Data Source
• Clients in the branch • Servers in the core (data center) • NAM in the core	Client	Server Server WAN
• Clients in the branch • Servers in the core (data center) • NAM in the core	Client Client WAN	Server
• Servers in the branch • Clients in the core (data center) • NAM in the core	Server	Client Client WAN
• Servers in the branch • Clients in the core (data center) • NAM in the branch	Server Server WAN	Client

Table 5-2 WAAS Deployment Scenarios (continued)

Deployment Scenario	Edge WAE Data Source	Core WAE Data Source
• Servers and clients in the branch and the core (data center) • NAM in the core	Client Server	Client Server Client WAN Server WAN
• Servers and clients in the branch and the core (data center) • NAM in the branch	Client Server Client WAN Server WAN	Client Server

Monitoring and Analyzing Traffic Using the NAM

The monitoring and analyzing traffic using the NAM feature provides intuitive workflows and interactive reporting capabilities.

The monitoring and analyzing dashboards allow you to view network traffic, application performance, site performance, and alarms at a glance. From there, you can isolate one area, for example an application with response time issues, and then drill down to the dashboard for further investigation.

The section contains the following topics:

- NAM Metrics, page 5-7
- Top Talkers Dashboards, page 5-8
- Throughput Dashboards, page 5-10
- Performance Analysis Dashboards, page 5-11

NAM Metrics

You can use the NAM to report a variety of metrics, depending on which data sources you are monitoring, as shown in Table 5-3.

Table 5-3 NAM Data Source Monitoring

Monitored WAAS Data Sources	Metrics Available
Monitoring Client Data Sources: monitor TCP connections between the client and the WAE device	• Total response time as experienced by the client • Total transaction time as experience by the client • Bandwidth usage (bytes/packets) before optimization • Number of transactions and connections • Network time separated into client-edge and edge-server times

Table 5-3 NAM Data Source Monitoring (continued)

Monitored WAAS Data Sources	Metrics Available
Monitoring WAN Data Sources: Monitor the TCP connections between edge and core WAE devices	• Bandwidth usage (bytes/packets) after optimization • Network time of the WAN segment
Monitoring Server Data Sources: Monitor TCP connections between core WAE devices and the servers	• Server response time (without proxy acceleration or caching server) • Network time between the core WAE device and the servers

You can also configure data sources from the core WAE. You can add the Server, Server-WAN, and Passthrough data sources to monitor application performance analytics as observed from the server LAN, WAN, and the client LAN.

Top Talkers Dashboards

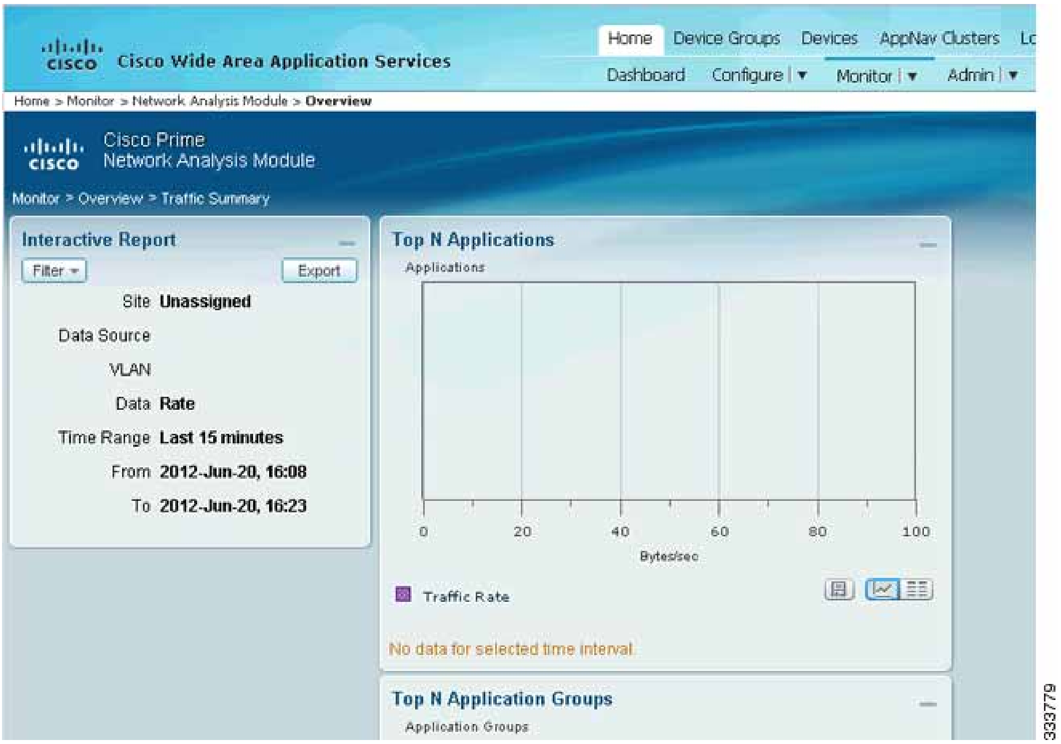
This section includes the following topics:

- Traffic Summary, page 5-8
- Top Talkers Details, page 5-10

Traffic Summary

The Top Talkers Summary dashboard allows you to view the Top N Applications, Top N Application Groups, Top N Hosts (In and Out), IP Distribution by Bytes, Top N DSCP, and Top N VLAN that is being monitored on your network. It provides auto-monitoring of traffic from all WAAS devices. You can view the Traffic Summary Dashboard by going to **Monitor** > **Network Analysis Module** > **Overview.** (See Figure 5-5).

Figure 5-5 NAM Monitoring Overview



Site Unassigned
Data Source
VLAN
Data Rate
Time Range Last 15 minutes
From 2012-Jun-20, 16:08
To 2012-Jun-20, 16:23

No data for selected time interval.

The charts shown on this dashboard are as follows:

- Top N Applications

  The Top N Applications Chart enables you to view the traffic rate (bytes per second or bits per second) or traffic volume (bytes or bits), depending on the Interactive Report filter selection (data rate or cumulative, respectively).

- Top N Application Groups

  This chart shows a detailed analysis of the Top N application groups and the traffic rate or volume for this interval.

- Top N Hosts (In and Out)

  This chart displays the traffic rate (bytes per second or bits per second) or traffic volume (bytes or bits).

- IP Distribution by Bytes

  This chart shows the percentages of bytes that are distributed to IP protocols (for example, IPv4 TCP).

- Top N DSCP

  This chart shows statistics for the top DSCP aggregation groups.

- Top N VLAN

  This chart shows the Top N VLAN statistics. In this chart, you might see VLAN 0, which is for traffic that does not have any VLAN tags.

Top Talkers Details

While you are in the process of deploying WAAS devices, you can get data to assist in the WAAS planning and configuration.

When you go to **Monitor > Network Analysis Module > Top Talkers Details**, you will see the window that assists you in the predeployment process. Use the Interactive Report window to select the traffic you want to analyze for optimization. The window displays the Top Applications, Top Network Links, Top Clients, and Top Servers.

Based on the results, you can then configure the WAAS products to optimize your network.

Throughput Dashboards

This section includes the following topics:

- Network, page 5-10
- Top Applications, page 5-10
- Application, page 5-11

Network

The Network dashboard enables you to view LAN versus WAN throughput for WAAS users both in the incoming and outgoing directions. To view these reports, configure interface groups that comprise WAN and LAN interfaces. The displayed information represents the total data collected since the collection was created or since the NAM was restarted. To view the Network dashboard, go to **Monitor > Network Analysis Module > Throughput > Network**.

Choose an interface group view from the Interface Selector on the left side of the window to see traffic in the charts. Click the arrow icon to the left of the NDE data source name to display all interfaces groups, and then select an interface group view. If the charts show no data, and you see the message "Interface needs to be selected," you have not yet chosen an interface group view.

After you choose the interface group view, you see the following charts populated:

- Interface Traffic (Ingress % Utilization and Egress % Utilization)
- Top N Applications—Ingress
- Top N Applications—Egress
- Top N Hosts—Ingress
- Top N Hosts—Egress
- Top N DSCP Aggr—Ingress
- Top N DSCP Aggr—Egress

You can enter the interface speed manually through the Interface capacity table, or the speed can be automatically configured if the SNMP settings for the NDE device are entered in the data source table.

Top Applications

In the Top Applications dashboard, you can view the top applications by the traffic rate over a selected time and for the specified site and/or data source.

Applications Over Time shows you all of the applications that have been running for the time period interval. The color-coded legend shows you what the applications are running.

Application

In the Application Analysis window, you can see the traffic level for a given application over a selected period of time. It is available under the **Monitor** > **Network Analysis Module** > **Throughput** > **Application**. This window shows you the following:

- A graph of application traffic over time.
- Top hosts that transmit and receive traffc on that application for the selected time period.
- Application Configuration that shows the criteria by which the NAM classifies packets as that application. This criteria is typically a list of TCP and/or UDP ports that identify the application. Some applications are identified by heuristic or other state-based algorithms.

Hosts Detail

On the "Top N Hosts - Traffic In" or "Top N Hosts - Traffic Out" chart, you can choose **Hosts Detail** to see the All Hosts window and the detailed information about all hosts. The All Hosts window displays the following information:

- Hos—Host address
- Application—Application type
- In Bytes/sec—Number of bytes per second incoming
- In Packets/sec—Number of packets per second incoming
- Out Bytes/sec—Number of bytes per second outgoing
- Out Packets/sec—Number of packets per second outgoing

Performance Analysis Dashboards

This section includes the following topics:

- Application, page 5-11
- Conversation Multisegments, page 5-12

Application

The Application dashboard provides the transaction time performance for an application as well as the original and optimized traffic volume reported by the flow agent. Information about how the transaction time is broken up across client, WAN, and server segments is also provided. For example, if the transaction time is dominated by the server segment time (due to a slow server), WAAS may not be able to improve the performance as much as when it is dominated by the WAN network time. To view the Application performance analysis dashboard, go to **Monitor** > **Network Analysis Module** > **Performance Analysis** > **Application**.

The charts available on this dashboard are as follows:

- Transaction Time (Client Experience)
- Traffic Volume and Compression Ratio

- Average Concurrent Connections (Optimized vs. Passthru)
- Multi-Segment Network Time (Client LAN - WAN - Server LAN)

Conversation Multisegments

The Conversation Multiple Segments dashboard correlates data from different data sources and allows you to view and compare response time metrics from multiple WAAS segments (data sources). To view the Conversation Multiple Segments dashboard, go to **Monitor > Network Analysis Module > Performance Analysis > Conversation Multisegments**.

The Response Time Across Multiple Segments window shows the response time metrics of the selected server or client-server pair from applicable data sources.