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 the WAAS environment.

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.

Monitoring WAAS Network Health

This section describes how to use WAAS Central Manager to monitor the health of the WAAS environment. 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

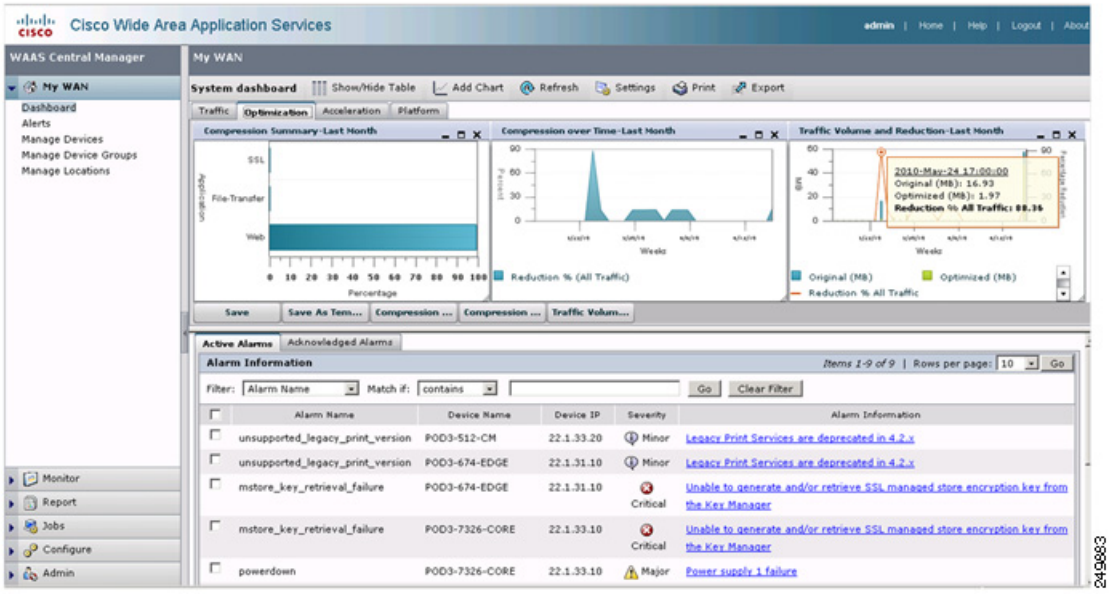
You must have proper username and password credentials to log in to WAAS Central Manager.

This section contains the following topics:

Using the WAAS Dashboard

You can view general and detailed information about your WAAS network by choosing My WAN > Dashboard. The System Dashboard window appears, which by default displays the Optimization tab (see Figure 1-1).

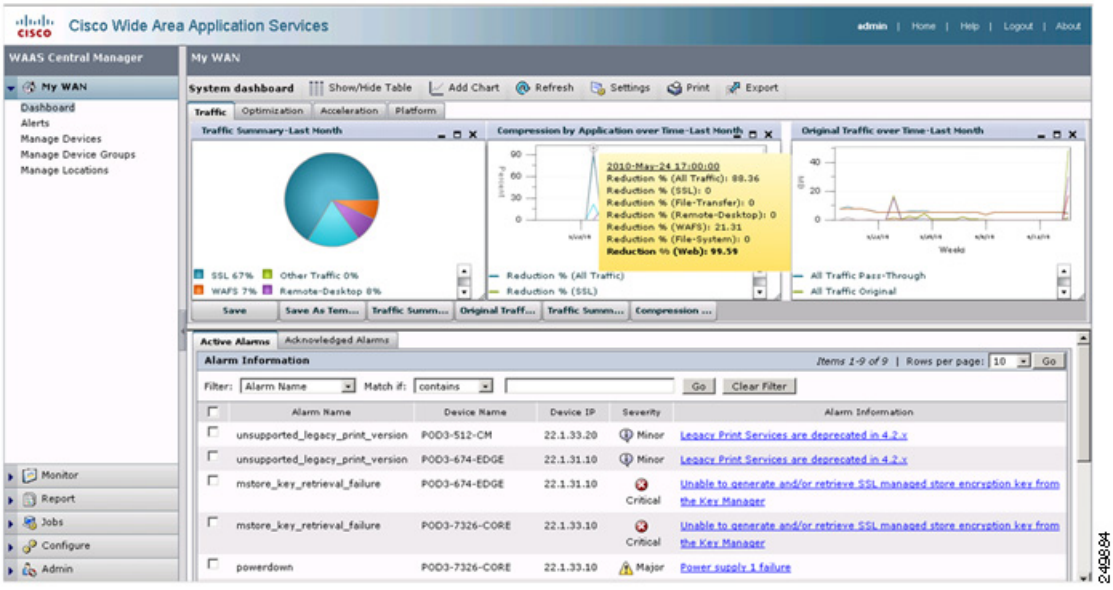
Figure 1-1 WAAS Central Manager: Dashboard Optimization Tab



The charts provide a snapshot of overall WAAS network health. Various reporting options are available from each tab. You can select charts and customize them for a specific time frame. Navigating over a chart or a cross point on a chart displays additional useful information.

Figure 1-2 shows a sample of the traffic dashboard which you can view by clicking the Traffic tab.

Figure 1-2 WAAS Central Manager: Dashboard Traffic Tab



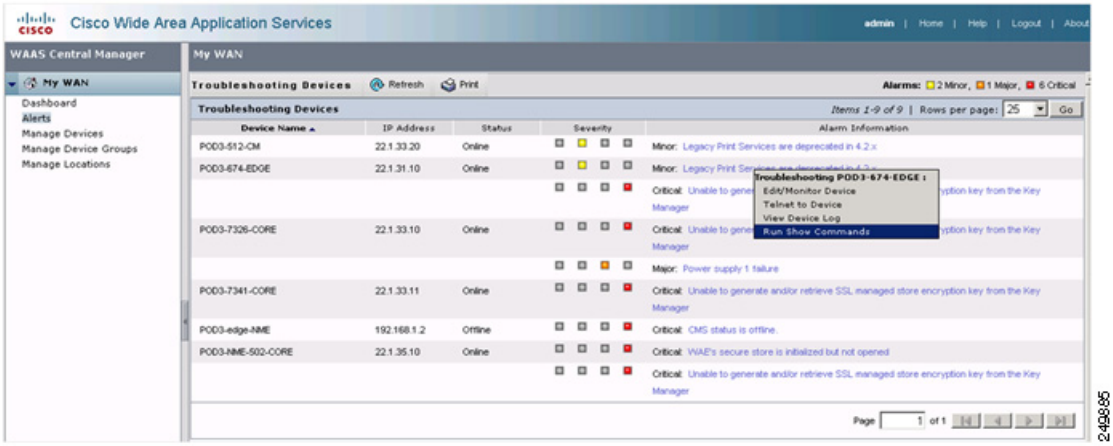
The dashboard also displays any network-wide alarms that may be present. Additional information is provided when you navigate to the alarm hyperlink or simply click it. From the Active Alarms tab, you can acknowledge alarms, which are then moved to the Acknowledged Alarms tab.

The alarms are classified as Critical, Major, or Minor depending on the impact the issue might have upon the WAAS environment. You can use the filter option to display alarms by severity, device IP address or name, and so forth. Filter match criteria is case sensitive.

Viewing Alarms

You can view alarms by choosing My WAN > Alerts. The Troubleshooting Devices window appears (see Figure 1-3).

Figure 1-3 WAAS Central Manager: Troubleshooting Devices



The screen provides a good overall view of outstanding alarms where you can take an action or acknowledge the alarms per device.

Common Alarms include:

Alarm 17001 (join_timeout) WCCP service join timeout.

Severity: Major

Category: Communications

Description: The device cannot join the WCCP service group within 10 minutes. Traffic redirection to the WAE cannot occur until the WAE can join.

Action: Restart the WCCP configuration by disabling WCCP on all the WAEs in the farm that present this alarm, waiting 5 minutes, and then reenabling WCCP on these WAEs.

Alarm 17002 (rtr_unreachable) WCCP Router Unreachable Alarm.

Severity: Major

Category: Communications

Description: The device cannot receive ISUs from the router for more than 30 seconds. Network connectivity between the router and WAE is down or the WCCP configuration on the WAE is not consistent with that of the router. This situation results in a failure to join the router in the WCCP farm.

Action: Check the configuration on the router and the WAE that raised the alarm. Check connectivity between the WAE and the router for which the alarm is raised.

Alarm 17003 (rtr_unusable) WCCP Router Unusable Alarm.

Severity: Minor

Category: Communications

Description: The device cannot join the WCCP farm due to mismatching capabilities. The assignment method, redirect method, or return method are not matching with the capability offered by the router.

Action: Check and modify the capability configuration on the WAE or the router to match the capability supported in the farm.

Alarm 17004 (missing_assignment) WCCP Missing Assignment alarm.

Severity: Major

Category: Communications

Description: The device has joined the WCCP farm but does not have any assignments. Traffic redirection to the device does not occur. The possible reasons for this to happen could be: 1) if using mask assignment, the mask value of the device is not consistent with the rest of the farm; 2) the device lost all assignments to other devices with higher weights in the farm; or 3) the device cannot communicate to all routers in the farm and thus is not given any assignments. The alarm is raised if the WAE does not acquire assignments within three minutes after a change in the farm.

Action: Check configuration and connectivity to all routers and take corrective action as needed.

Alarm 17005 (mask_mismatch) Configured mask mismatch for WCCP.

Severity: Major

Category: Communications

Description: The device cannot join the WCCP farm because its configured mask does not match the operational mask of the farm. Traffic redirection to the WAE cannot occur until the WAE can join.

Action: Check the WCCP mask configuration on all WAEs to ensure that they are configured with the same mask.

Alarm 330001 (svcdisabled) -service name- service has been disabled.

Severity: Critical

Category: Processing

Description: The node manager tried restarting the specified service but the service kept restarting. The number of restarts has exceeded an internal limit and the service has been disabled.

Action: The device may have to be reloaded for the service to be reenabled.

Alarm 330002 (servicedead) -service name- service failed.

Severity: Critical

Category: Processing

Description: A critical service has failed. Attempts will be made to restart this service but the device may run in a degraded state.

Action: The device could reboot itself to avoid instability. Examine the syslog for messages relating to cause of service failure.

Alarm 335000 (alarm_overload) Alarm Overload State has been entered.

Severity: Critical

Category: Quality of service

Description: The Node Health Manager issues this to indicate that the device is raising alarms at a rate that exceeds the overload threshold.

Action: Access the device and determine what services are raising the alarms. Take corrective action to resolve the issues with the individual services.

Alarm 335001 (keepalive) Keepalive failure for -application name-. Timeout = n seconds.

Severity: Critical

Category: Quality of service

Description: The Node Health Manager issues this message to indicate that an application has not issued a keepalive to the Node Health Manager for the last *n* seconds. The application's health is in question.

Action: Access the device and determine what state the specific application is in. Take corrective action to resolve the issues that are keeping the application from running properly.

Alarm 445000 (disk_failure) A disk has failed.

Severity: Critical

Category: Equipment

Description: The System Monitor issues this message to indicate that one of the disks attached to a device has a severe error.

Action: Access the device and execute the **show disk details** CLI command. If the problem persists, replace the disk.

Alarm 445001 (core_dump) A user core file has been generated.

Severity: Major

Category: Processing

Description: The System Monitor issues this to indicate that one or more of the software modules has generated a core file.

Action: Access the device, check the directory /local1/core_dir, retrieve the core file through FTP, and contact Cisco TAC.

Alarm 445013 (powerdown) Power supply is down.

Severity: Major

Category: Processing

Description: The System Monitor indicates that one of the power supplies is down.

Action: Check the power supplies.

Alarm 445019 (license_failure) WAAS product license is missing.

Severity: Critical

Category: Processing

Description: The System Monitor indicates that either the WAAS product license has not been purchased or the License Management system has not been configured.

Action: Execute the **show license** CLI command to verify that the License Management system has been configured. Purchase the WAAS product license and configure the License Management system with the **license add** command.

Alarm 445022 (eth_detection_failed) Detection of one of the network interfaces has failed.

Severity: Critical

Category: Equipment

Description: The System Monitor indicates that the system networking hardware has a severe error. Interfaces and related features will not work properly.

Action: Reboot the device. If the alarm does not clear, reset the BIOS settings to the defaults before rebooting again. If the alarm does not clear, contact Cisco TAC.

Alarm 700002 (cms_clock_alarm) Device clock is not synchronized with the primary CM.

Severity: Major

Category: Environment

Description: If this device is a WAE, its clock needs to be synchronized with the primary WAAS Central Manager to make time-sensitive features like statistics, status monitoring, and event scheduling work correctly. If this device is a standby WAAS Central Manager, its clock needs to be synchronized with the primary WAAS Central Manager to make the WAAS Central Manager failover work.

Alarm 700006 (cms_wae_secure_store) Secure Store is initialized but not opened.

Severity: Critical

Category: Environment

Description: The WAE's secure store is initialized but not opened by the user. The WAE will reject updates from WAAS Central Manager if they contain updates to preposition, dynamic share, and WAFS core password and user configuration until the secure store is opened.

Action: Open secure store using the **cms secure-store open** CLI command or by entering the password in the WAAS Central Manager GUI.

Alarm 700008 (mstore_key_retrieval_failure) CMS/Management agent failed to generate and/or retrieve SSL managed store encryption key from Key Manager.

Severity: Critical

Category: Processing

Description: This alarm indicates one of following issues:

- The WAAS Central Manager device is not reachable
- Secure store on WAAS Central Manager is initialized but not open
- The Key Manager process on the WAAS Central Manager device is not running or failing to respond
- Key Manager cannot process key generation or retrieval request. If this issue is present, the WAAS device cannot process a configuration update received from WAAS Central Manager if it contains SSL certificate and key pair information.

Action: Check to see if the WAAS Central Manager device is reachable (TCP connections from the WAE to the WAAS Central Manager on port 443). Check the following log files for additional information about the error:

- On WAE: /local1/errorlog/kc.log on WAE
- On WAAS Central Manager: /local1/errorlog/km/km.log

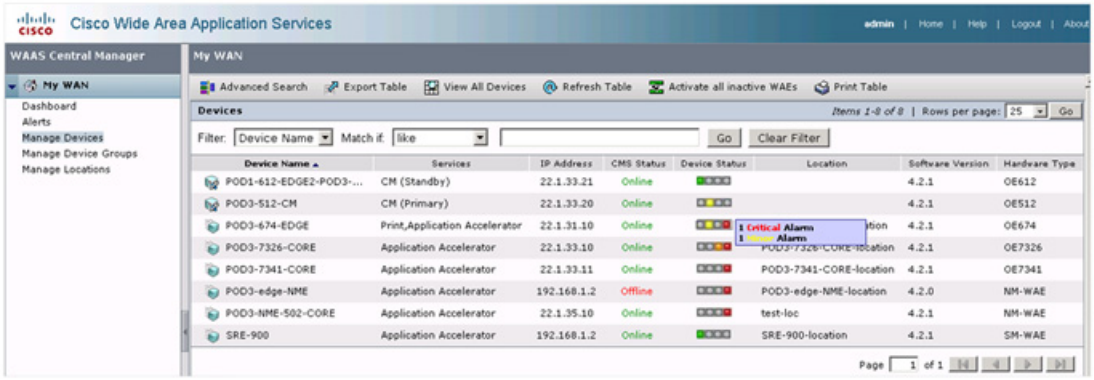
Action: Fix the clock on the device or the primary WAAS Central Manager.

For a complete list of alarm conditions, see the *Alarm Book* located in the WAAS 4.2.1 Software Download area on Cisco.com.

Viewing WAE Device Status

The Cisco WAAS Central Manager devices page provides a quick status overview of each Cisco WAE deployed throughout the network that is registered against that particular WAAS Central Manager. You can manage devices by choosing My WAN > Manage Devices. The Devices window appears (see Figure 1-4).

Figure 1-4 WAAS Central Manager: Manage Devices



Each device reports a CMS Status of either online or offline, which alerts the administrator to the state of the Cisco WAE at that time. If the Central Management System (CMS) service is disabled or network connectivity is unavailable to that particular Cisco WAE, it is reported as offline. WAAS Central Manager cannot synchronize configuration data with an offline Cisco WAE and cannot fetch new reporting data.

If a device shows up as offline, confirm the status by using telnet or SSH to access the device and entering the **show cms info** command. In addition, you should use commands such as **show stat connection** to verify that the device is participating in traffic optimization.

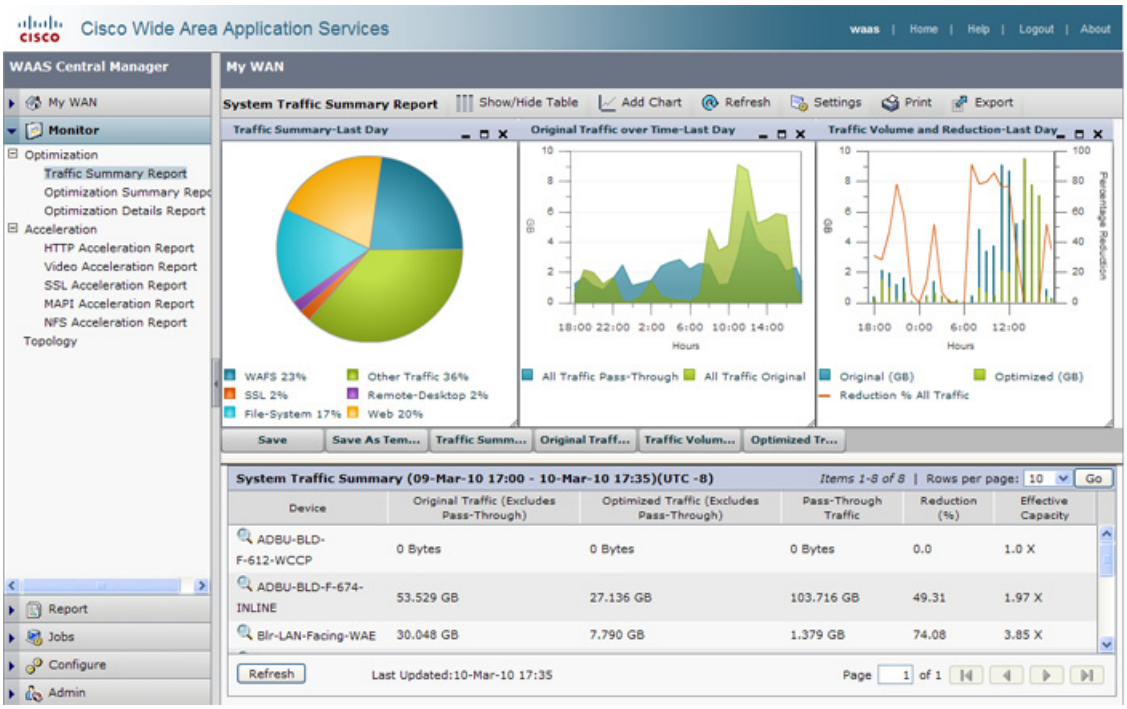
The Devices window also presents some key information such as device name, service mode, IP address, software version, and so forth. Ideally, all the WAEs in the WAAS network should be running the same OS version. At a minimum, the primary WAAS Central Manager and secondary WAAS Central Manager (if there is one) should be on the same version.

Device health is indicated by the device status highlighting any outstanding alarms. You can navigate to the device by clicking on the device icon. For large deployments, use the Filter option to display devices by device name, service mode, and status.

Monitoring Optimization

You can access system-wide traffic statistics by choosing My WAN > Monitor > Optimization > Traffic Summary Report. The System Traffic Summary Report window appears (see Figure 1-5).

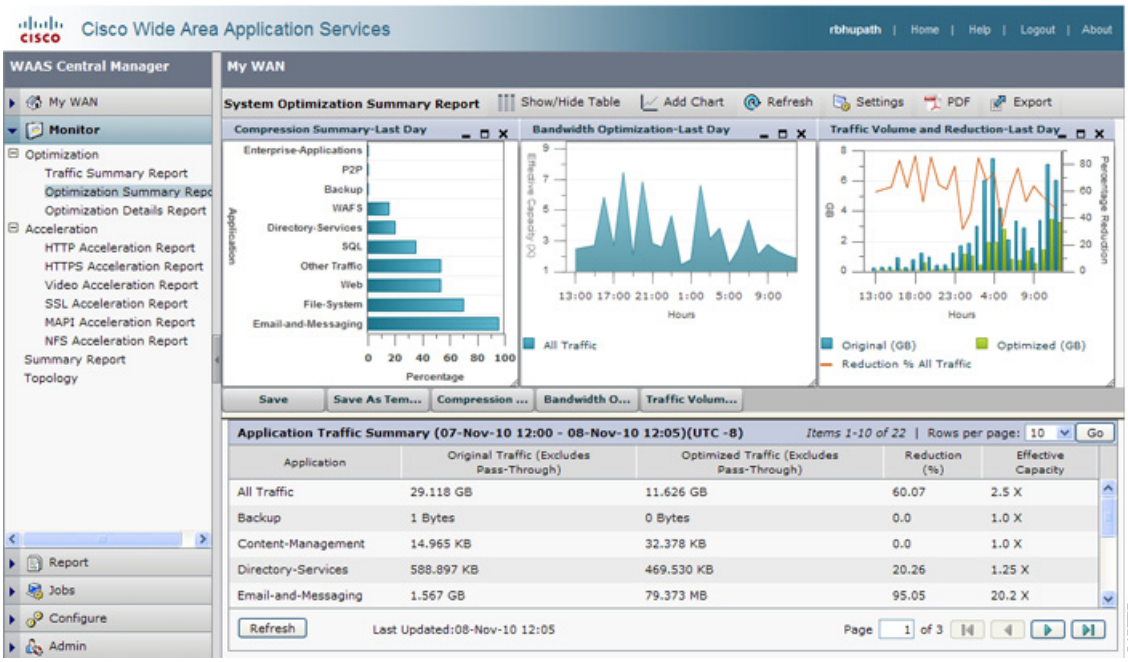
Figure 1-5 WAAS Central Manager: System Traffic Summary Report



Several reporting options are available for both optimization and protocol specific application accelerator acceleration reporting. The System Traffic Summary table provides device-level optimization statistics that are useful to determine if the WAAS devices are configured properly for optimal traffic acceleration.

You can access system-wide optimization statistics by choosing My WAN > Monitor > Optimization > Optimization Summary Report. The System Optimization Summary Report window appears (see Figure 1-6).

Figure 1-6 Optimization Summary Report



The System Optimization report provides application level optimization reports, highlighting reduction and effective capacity. You can use this data to modify policies and adjust optimization options.

The Acceleration reports provide device-level application accelerator specific statistics.

Monitoring System Operation

You can monitor the system operation by choosing My WAN > Monitor > Summary Report. The Summary Report displays.

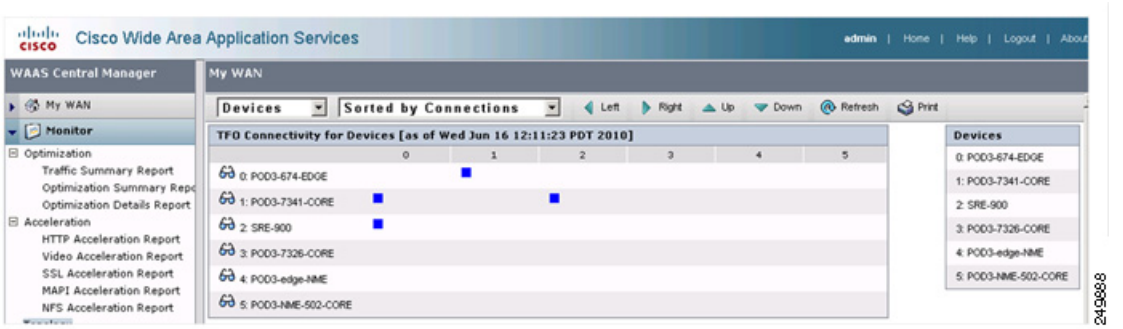
Figure 1-7 Summary Report

The Summary report is a predefined report that can be used to monitor the system operation. The Summary Report can be customized to display the charts that you require. Use the Add Chart option to select the charts that you want to be displayed on this report. Only 12 charts can be displayed in the report. You can customize any of the chart settings by using the Settings option.

Monitoring Topology

You view peering relationships by choosing My WAN > Monitor > Topology. The TFO Connectivity for Devices window appears (see Figure 1-8). A bidirectional relationship is required for any optimization between the peers.

Figure 1-8 WAAS Central Manager: TFO Connectivity for Devices

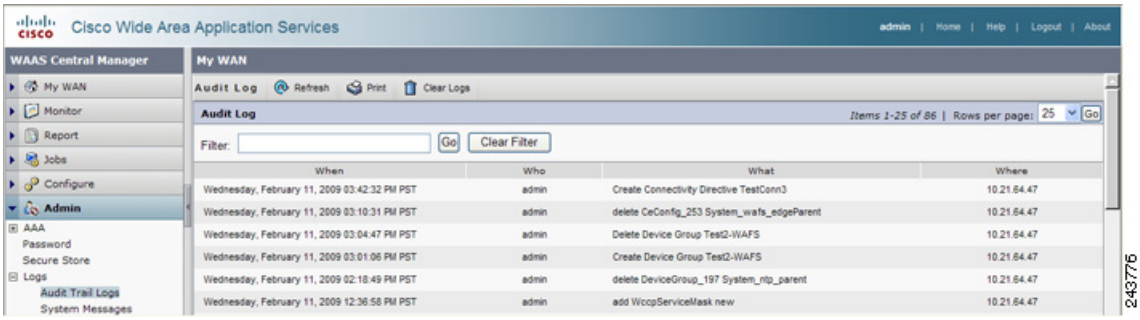


The topology information is important for troubleshooting and for deployment sizing exercises, especially for large deployments where any site-to-site communication is required.

Monitoring Audit Trail Logs, System Messages, and WAAS Central Manager Logs

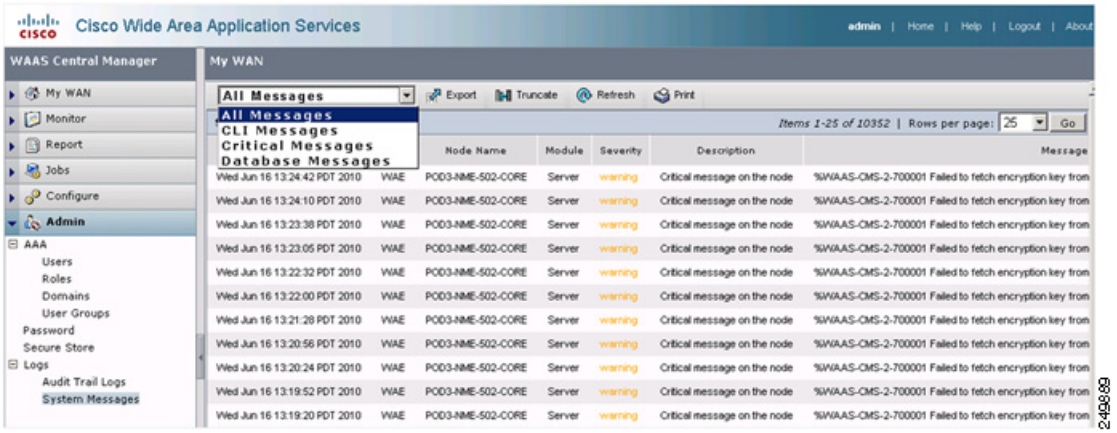
You can view the Audit Trail Logs to track the last actions performed by a particular user that you created using the WAAS Central Manager GUI, which can be used to centrally create and manage two different types of administrator user accounts (device-based CLI accounts and roles-based accounts) for your WAAS devices. To view the Audit Trail Logs, choose My WAN > Admin > Logs > Audit Trail Logs. The Audit Trail Logs window appears (see Figure 1-9).

Figure 1-9 WAAS Central Manager: Audit Trail Logs



You can view system wide-system logs by choosing My WAN > Admin > Logs > System Messages. The System Messages window appears (see Figure 1-10). You can choose the system messages to view CLI, critical, or database messages.

Figure 1-10 WAAS Central Manager: System Messages



For a complete list of available errors, see the *Error Message Book* in the WAAS 4.2.1 Software Download area on Cisco.com.

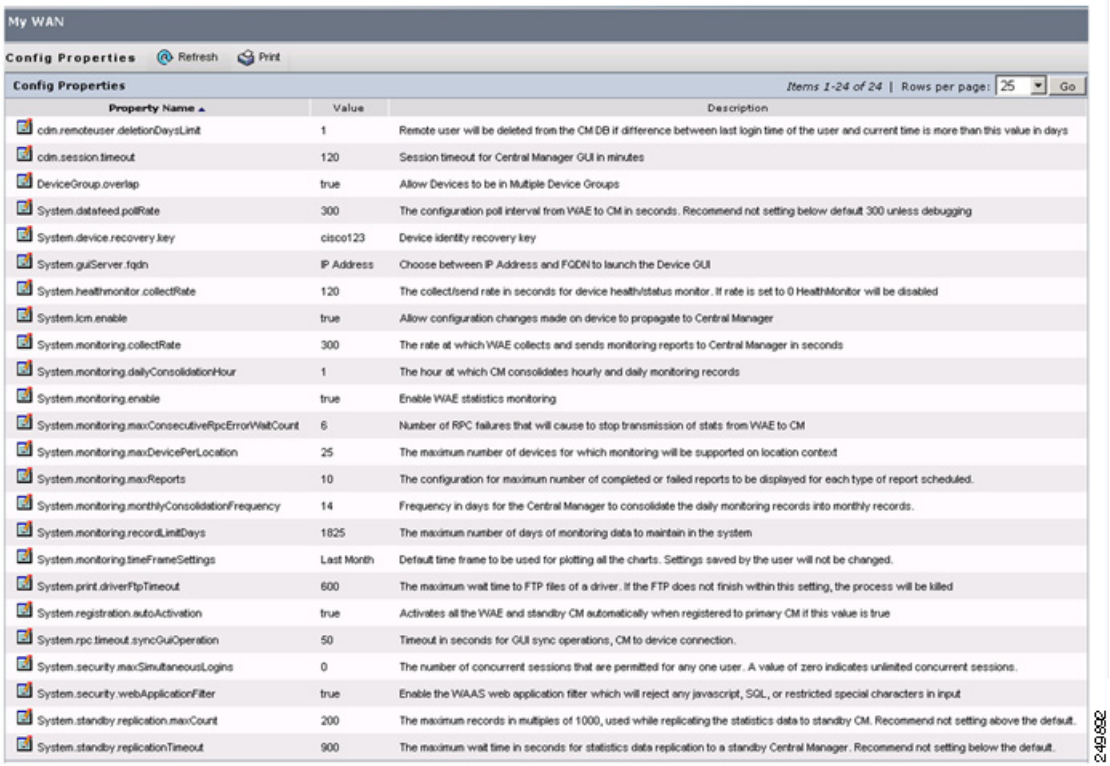
You can view the WAAS Central Manager logs by choosing My WAN > Devices > WAAS-CM > Admin > Logs. The System Messages Log window appears (see Figure 1-11).

Figure 1-11 Figure 8: WAAS Central Manager: System Messages Log

Viewing System Properties

You can view and modify the current system properties by choosing My WAN > Configure > System Properties. The Config Properties window appears (see Figure 1-12). From this window, you can modify the preconfigured system properties to alter the default behavior of the system. For more information, see the *Cisco Wide Area Application Services Configuration Guide* chapter on "Configuring Other System Settings."

Figure 1-12 WAAS Central Manager: System Properties



Monitoring WAAS Device Health

You can use WAAS Central Manager to monitor and configure all devices in the WAAS network. WAAS Central Manager provides detailed information about a WAAS device configuration, device hardware statistics, and traffic optimization reports.

This section contains the following topics:

Viewing the Device Dashboard

You can manage devices individually by choosing My WAN > Devices > *Device_Name*. The Device Dashboard window appears (see Figure 1-13).

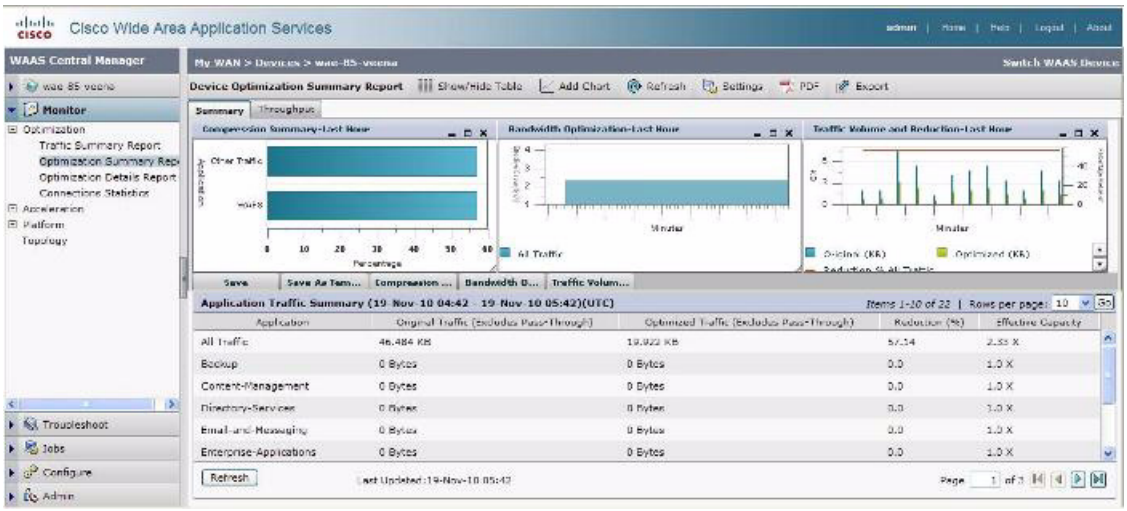
Figure 1-13 WAAS Central Manager: Device Dashboard

The Device Dashboard provides an overview of the device, such as the WAAS hardware and software, and the configured interception mechanism. You can customize the charts and save the custom settings. You can also access the device GUI or telnet to the device.

Viewing Optimization Reports

You can view optimization reports by choosing My WAN > Devices > *Device_Name* > Monitor > Optimization > Optimization Summary Report. The Device Optimization Summary Report window appears (see Figure 1-14).

Figure 1-14 WAAS Central Manager: Device Optimization Summary Report



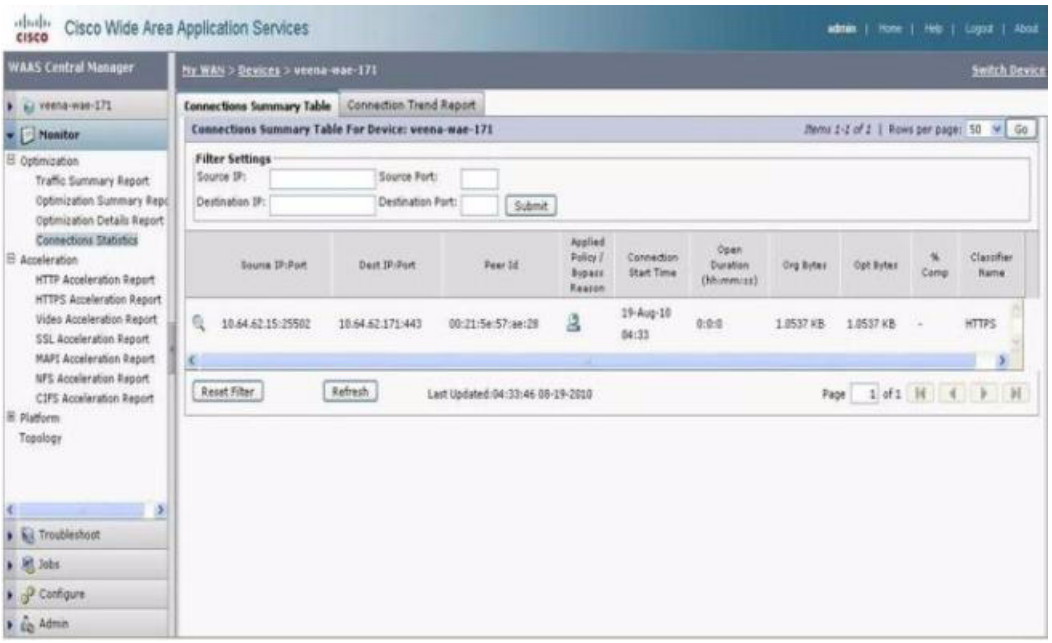
This report includes Summary and Throughput reports. These are optimization reports that provide traffic optimization statistics for predefined applications and insight into which applications are getting the most optimization and which ones may need additional fine tuning.

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

Viewing Connection Statistics

You can view per-connection statistics by choosing My WAN > Devices > *Device_Name* > Monitor > Optimization > Connection Statistics. The Connection Statistics report displays the device's Connections Summary Table (see Figure 1-15) and a Connection Trend Report (see Figure 1-15).

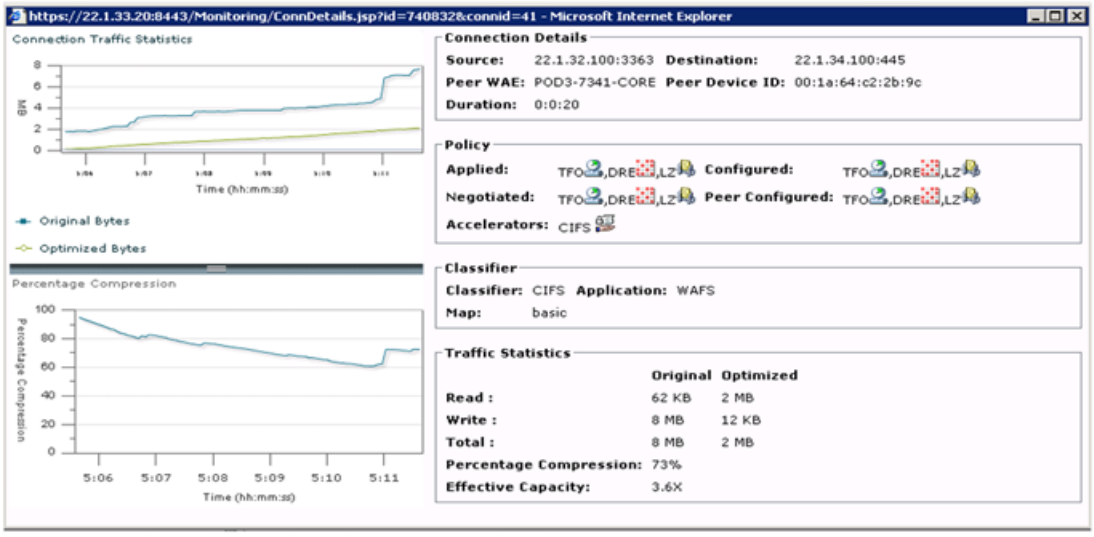
Figure 1-15 WAAS Central Manager: Connections Summary Table



The Connections Summary Table lists all the active flows 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.

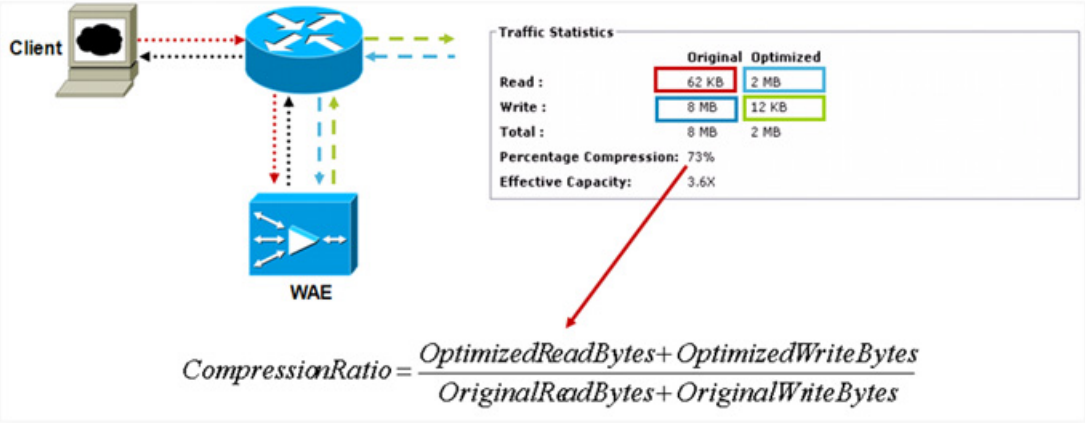
To view additional details per flow, click the magnifying glass icon. The flow details pop-up window opens, which provides connection statistics over time that can be used for troubleshooting or reporting (see Figure 1-16). This pop-up window updates automatically.

Figure 1-16 WAAS Central Manager: Flow Details Pop-Up Window



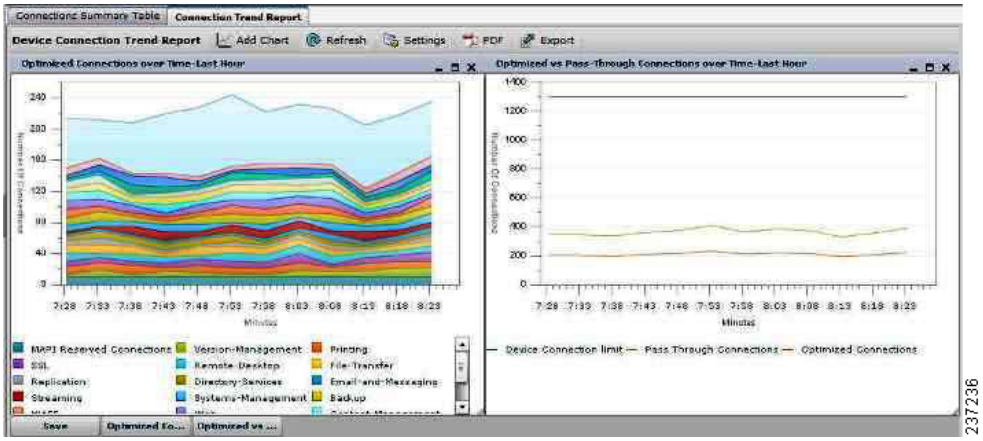
The traffic statistics provides compression ratios, effective capacity, and byte values for the original and optimized sockets. Figure 1-17 illustrates how to interpret the displayed data.

Figure 1-17 Interpreting Traffic Statistics



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.

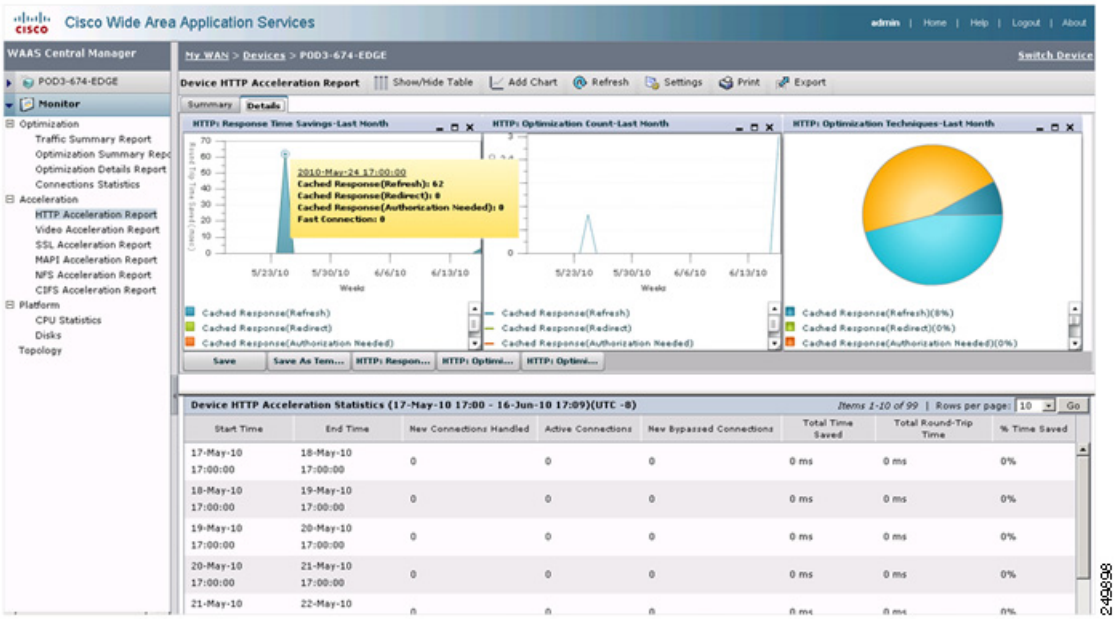
Figure 1-18 Connection Trend Report



Viewing Accelerations Reports

You can view acceleration reports for any application optimizer by choosing My WAN > Devices > *Device_Name* > Monitor > Acceleration > HTTP Acceleration Report. The Device HTTP Acceleration Report window appears (see Figure 1-19).

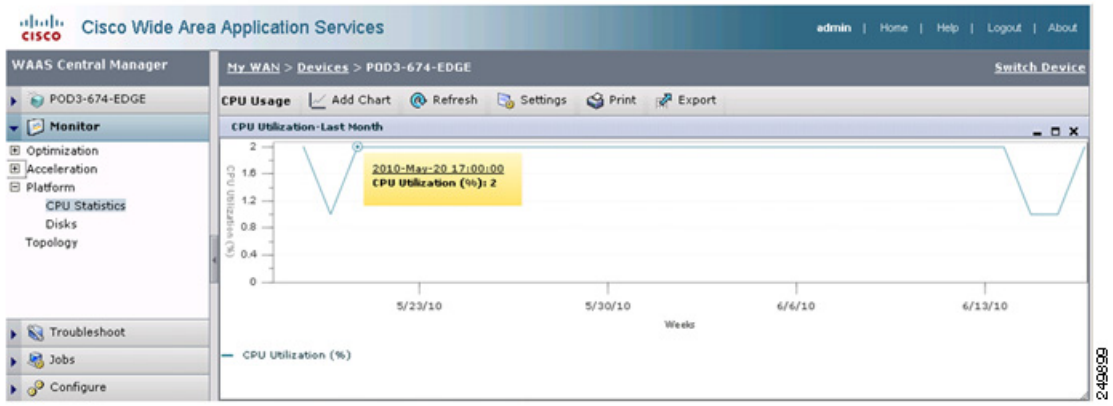
Figure 1-19 WAAS Central Manager: Device HTTP Acceleration Report



Viewing CPU Statistics

You can view WAAS device CPU utilization by choosing My WAN > Devices > *Device_Name* > Monitor > Platform > CPU Statistics. The CPU Usage window appears (see Figure 1-20).

Figure 1-20 WAAS Central Manager: CPU Usage

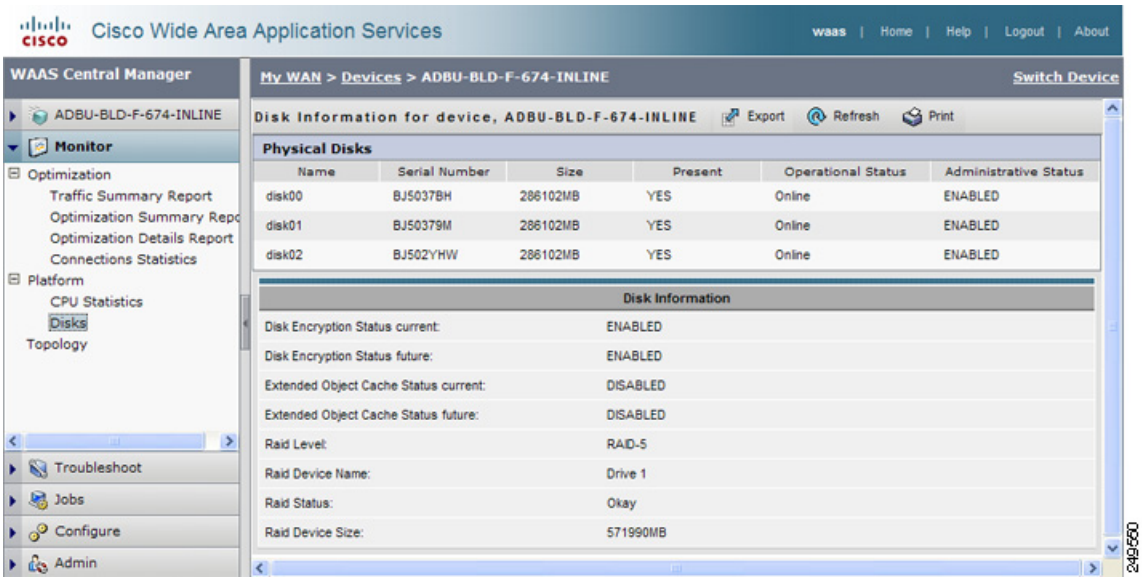


For a more complete view, change the CPU graph time length to a week or month. High CPU usage does not necessarily mean that there is an issue; it should be looked at in combination with other statistics to rule out any degradation in optimization. Other factors to consider include degradation in optimization or low compression, and so forth.

Viewing Disk Health and Status

You can check the disk status for an individual WAE by choosing My WAN > Devices > *Device_Name* > Monitor > Platform > Disk. The device Disk Information window appears (see Figure 1-21).

Figure 1-21 WAAS Central Manager: Disk Information



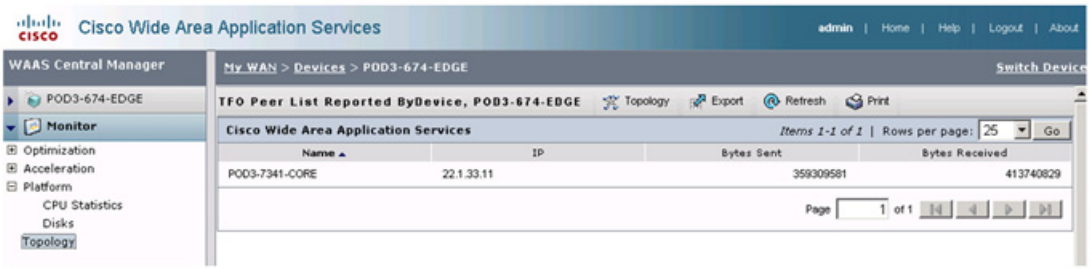
The operational status can be Online, Defunct, Missing, <null>, or Rebuilding. Under normal working conditions, the operation status should be Online. The Rebuilding status indicates that the RAID pairing is in progress and should clear after a while (depending on disk size and hardware platform of the WAE).

The view also displays disk size, RAID, disk encryption, and extended CIFS cache feature status.

Viewing Device Peering Status

You can view the device peering status at any given time to validate the traffic flows and optimal acceleration for these traffic flows by choosing My WAN > Devices > *Device_Name* > Monitor > Topology. The device TFO Peer List window appears (see Figure 1-22).

Figure 1-22 WAAS Central Manager: TFO Peer List



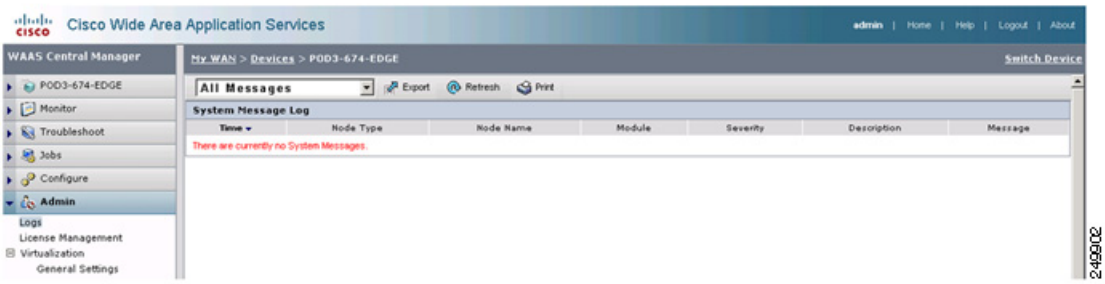
The peer list provides details about data sent and received for each peer. Branch site WAEs should have higher received numbers because all the traffic should be flowing from the data center towards the branch sites.

To view the overall topology, click the Topology icon.

Viewing Device Logs

You can view the device logs by choosing My WAN > Devices > *Device_Name* > Admin > Logs. The System Message Log window appears (see Figure 1-23).

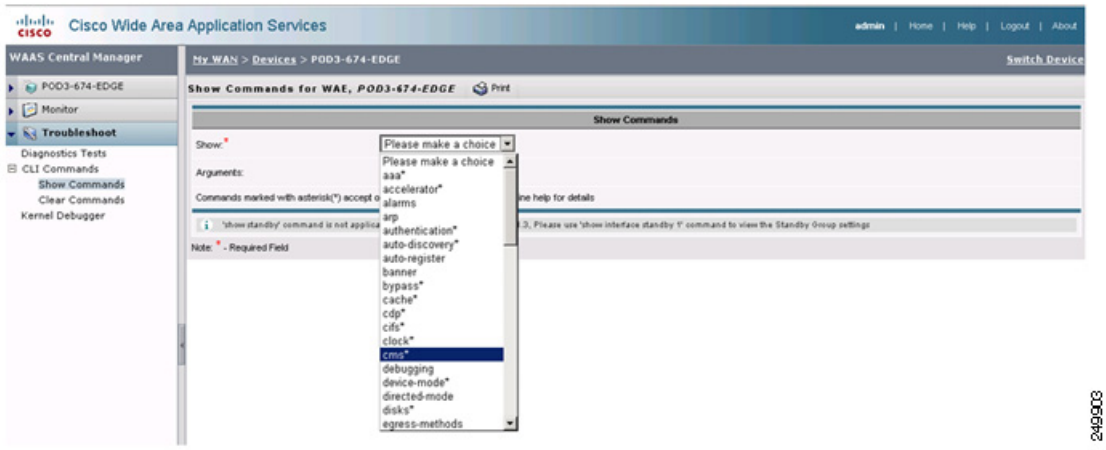
Figure 1-23 WAAS Central Manager: System Message Log



Running CLI Commands from the WAAS Central Manager GUI

You can run various CLI **show** commands to display additional useful information by choosing My WAN > Devices > *Device_Name* > Troubleshoot > CLI Commands > Show Commands. The Show Commands for WAAS window appears (see Figure 1-24).

Figure 1-24 WAAS Show Commands



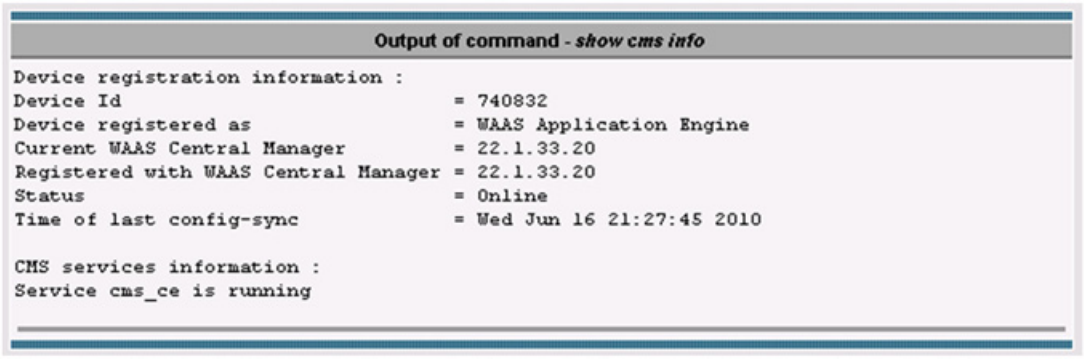
To display a command output, from the command drop-down list, select the **show** command and specify any optional command arguments. The output displays in a pop-up window. The sections that follow describe the output of some of the **show** commands. For details about the command options and output, see the *Cisco Wide Area Application Services Command Reference*.

This section contains the following topics:

show cms info Command Output

The **show cms info** command output provides the WAE registration information along with the last configuration synchronization time with WAAS Central Manager, which is useful when you suspect an application policy configuration issue (see Figure 1-25).

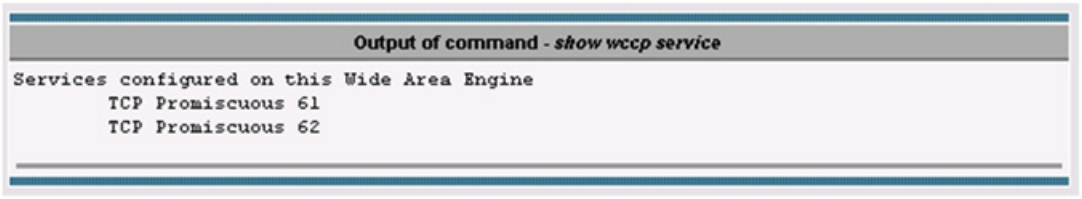
Figure 1-25 Command Output: show cms info



show wccp service Command Output

The **show wccp service** command output indicates if the WAE is configured for service groups 61 and 62 (see Figure 1-26).

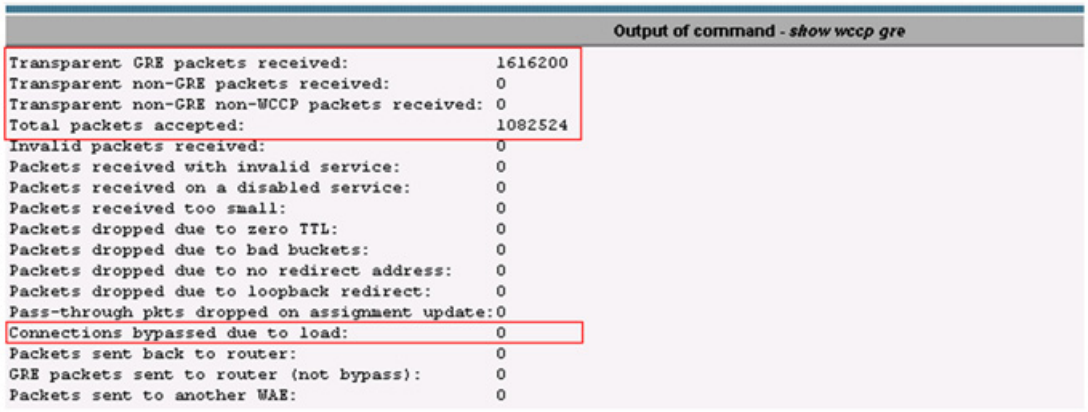
Figure 1-26 Command Output: show wccp service



show wccp gre Command Output

The **show wccp gre** command output includes three packets received counters, one of which should be incrementing to indicate that the WAE is receiving redirected packets (see Figure 1-27).

Figure 1-27 Command Output: show wccp gre



If the device is under heavy load and no new flows can be optimized, the Bypass Due to Load counter increments. A non-zero value for this counter indicates that the device is under overload or has gone in overload and should be further investigated.

show statistics connection Command Output

The **show statistics connection** command output displays the current optimized, auto-discovery, pass-through, and reserved flows (see Figure 1-28). The reduction ratio also displays for each active connection.

Figure 1-28 Command Output: show statistics connection

Output of command - *show statistics conn*

```
Current Active Optimized Flows:                        3
   Current Active Optimized TCP Plus Flows:            1
   Current Active Optimized TCP Only Flows:            1
   Current Active Optimized TCP Preposition Flows:     0
Current Active Auto-Discovery Flows:                   0
Current Reserved Flows:                                15
Current Active Pass-Through Flows:                     0
Historical Flows:                                      28


D:DRE,L:LZ,T:TCP Optimization RR:Total Reduction Ratio
A:AOIM,C:CIFS,E:EPM,G:GENERIC,H:HTTP,M:MAPI,N:NFS,S:SSL,V:VIDEO

ConnID         Source IP:Port           Dest IP:Port             PeerID Accel RR
     1      22.1.34.100:42300      22.1.32.100:3389 00:1a:64:c2:2b:9c T     00.0%
     2      22.1.34.100:42308      22.1.31.10:50139 00:1a:64:c2:2b:9c TDL   48.4%
    11       22.1.32.100:4009       22.1.34.100:445 00:1a:64:c2:2b:9c TCDL  12.4%
```

249907

To view additional details for each flow, include the optional **conn-id** argument as follows:

show statistics connection conn-id *conn-id-number*

show statistics connection optimized cifs Command Output

The **show statistics connection optimized cifs** command output displays the connection optimized by the CIFS application accelerator (see Figure 1-29).

Figure 1-29 Command Output: show statistics connection optimized cifs

Output of command - *show statistics connection opt cifs*

```
Current Active Optimized Flows:                        3
   Current Active Optimized TCP Plus Flows:            1
   Current Active Optimized TCP Only Flows:            1
   Current Active Optimized TCP Preposition Flows:     0
Current Active Auto-Discovery Flows:                   0
Current Reserved Flows:                                15
Current Active Pass-Through Flows:                     0
Historical Flows:                                      28


D:DRE,L:LZ,T:TCP Optimization RR:Total Reduction Ratio
A:AOIM,C:CIFS,E:EPM,G:GENERIC,H:HTTP,M:MAPI,N:NFS,S:SSL,V:VIDEO

ConnID         Source IP:Port           Dest IP:Port             PeerID Accel RR
    11       22.1.32.100:4009       22.1.34.100:445 00:1a:64:c2:2b:9c TCDL  12.3%
```

249908

show statistics accelerator cifs detail Command Output

The **show statistics accelerator cifs detail** command output displays statistics for the CIFS application accelerator, which is useful when troubleshooting connections handled by the CIFS application accelerator (see Figure 1-30).

Figure 1-30 Command Output: show statistics accelerator cifs detail

Output of command - *show statistics accelerator cifs det*

```
CIFS:
   Global Statistics
   -----------------
   Time Accelerator was started:                                  Sat Jun  5 05:48:47 2010
   Time Statistics were Last Reset/Cleared:                       Sat Jun  5 05:48:47 2010
   Total Handled Connections:                                     7
   Total Optimized Connections:                                   3
   Total Connections Handed-off with Compression Policies Unchanged:  0
   Total Dropped Connections:                                     0
   Current Active Connections:                                    1
   Current Pending Connections:                                   0
   Maximum Active Connections:                                    3
   Number of local reply generating requests:                     9716
   Number of remote reply generating requests:                    7930
   The Average time to generate a local reply (msec):             3
   Average time to receive remote reply (ms):                     10503
```

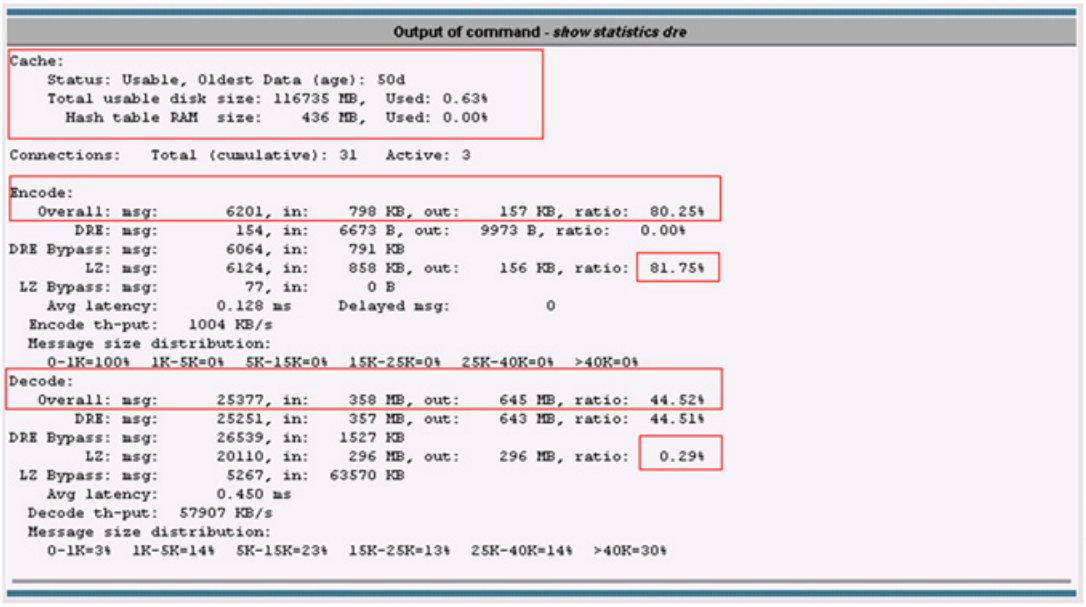
249909

The output highlights current active flows and historic flows handled by the application accelerator. Depending on the application accelerator, additional information is available that indicates application-specific optimization details.

show statistics dre Command Output

The **show statistics dre** command output displays the compression ratios for both encode and decode and includes details about DRE age, cache size available, and used percentage (see Figure 1-31).

Figure 1-31 Command Output: show statistics dre

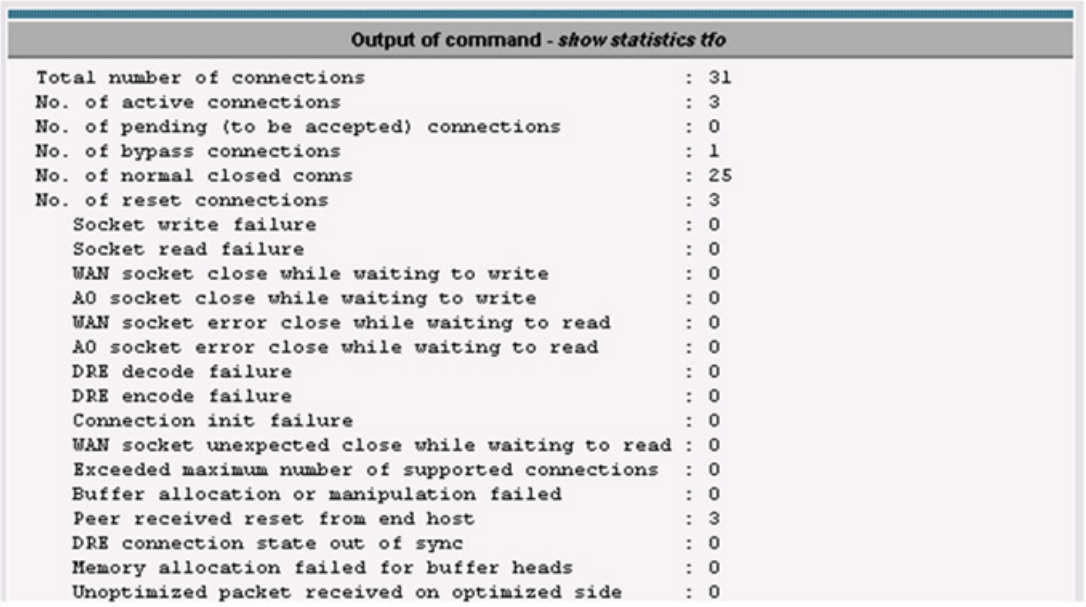


The output also includes LZ compression ratios for both encode and decode.

show statistics tfo Command Output

The **show statistics tfo** command output displays total, active, pending and bypass connection counts handled by the WAE (see Figure 1-32).

Figure 1-32 Command Output: show statistics tfo



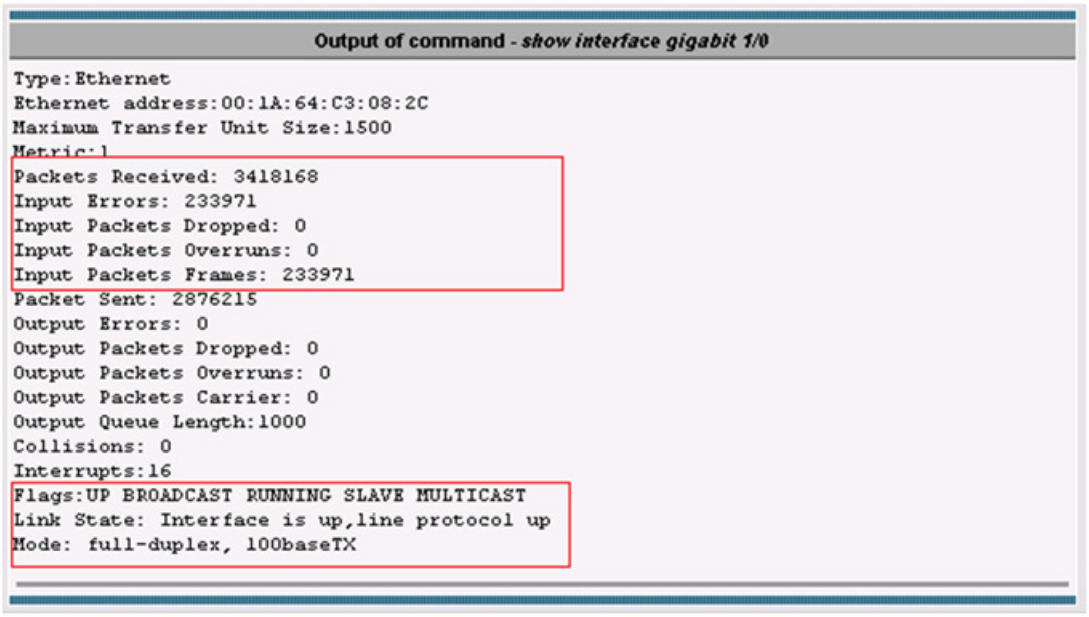
The output also provides connection reset counts that indicate the cause of a connection reset.

Note Pay special attention to the connection reset counter because it may indicate a problem outside the WAAS appliance.

show interface gig 1/0 Command Output

The **show interface gig 1/0** command output indicates the interface status, speed/duplex, packets sent and received, and any errors encountered (see Figure 1-33).

Figure 1-33 Command Output: show interface gig I10



A speed and duplex mismatch is one of the most common reasons for poor performance.

show tech-support Command Output

The **show tech-support** command output displays key outputs for various CLI commands and can be used for monitoring and troubleshooting tasks (see Figure 1-34).

Figure 1-34 Command Output: show tech-support